IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	David E. MCDYSAN et al.	Conf. No.:	7593
Application No.:	09/723,501	Examiner:	Gold, A.
Filed:	November 28, 2000	Group Art Unit:	2157
Customer No.:	25537		
Attorney Docket No.:	RIC00043		
Client Docket No.:	09710-1236		

For: EXTERNAL PROCESSOR FOR A DISTRIBUTED NETWORK ACCESS SYSTEM

Assistant Commissioner for Patents
Alexandria, VA 22313-1450

DECLARATION UNDER 37 CFR 1.131

Dear Sir:

We, Dave McDysan, Howard Lee Thomas, and Lei Yao, declare as follows:

1. We were employed by MCI, Inc., now an affiliate of Verizon Communications, Inc., assignee in interest for the subject matter of the above-referenced patent application, U.S. Application Serial Number 09/723,501, when the invention was conceived in this country and when the application was subsequently filed on November 28, 2000. In that capacity, we have personal knowledge of the facts and circumstances stated herein, except those statements which are made upon information and belief as set forth below.

2. We are joint inventors of the above-referenced patent application (Exhibit N).

3. It is our understanding that an Office Action mailed January 13, 2006 for the present application rejected claims 2-6, 9, 20-24, 27, 37, and 38 under 35 U.S.C. § 102(e) as anticipated by *Miles et al.* (U.S. 6,665,495) and rejected claims 7-8, 10-18, 25-26, 28-36 as obvious under 35 U.S.C. § 103(a) based, at least in part, on *Miles et al.*

4. We conceived our invention in this country long prior to October 27, 2000 (hereinafter the effective date), the effective filing date of U.S. Patent No. 6,665,495 entitled "Non-Blocking, Scalable Optical Router Architecture and Method for Routing Optical Traffic" to Miles et al.

5. Long prior to October 27, 2000, we prepared a description of our invention, a copy of which is attached hereto (Exhibit A). Although the dates of inventor signatures, headers, footers, and additional descriptive material has been redacted, we attest that the description was prepared long prior to the effective date of October 27, 2000.

6. Prior to October 27, 2000, and through November 28, 2000, we collaborated with Attorneys Brian Russell and Paul Roberts at least by telephone and email in their preparation of drafts of the above-referenced patent application, to review the drafts and suggest revisions, as evidenced at least by Exhibits B - L, in which page headers and footers, internal numbers, telephone numbers, email addresses, names of people copied on correspondence, and dates and times have been redacted.

7. Exhibit E denotes an email message dated August 31, 2000 from Attorney Brian Russell to co-inventor Lei Yao explaining that a draft application was almost complete for co-inventor review.

8. Exhibit D denotes an email message dated September 5, 2000 from co-inventor Lei Yao to Attorney Brian Russell acknowledging receipt of the email of Exhibit E.

9. Exhibit C denotes an email message dated September 5, 2000 from Attorney Brian Russell to co-inventor Lei Yao reporting an attached draft application for co-inventor review.

10. Exhibit B denotes an email message dated October 5, 2000 from co-inventor Lei Yao to Attorney Brian Russell reporting attached consolidated co-inventor comments on a draft application.

11. Exhibit F denotes an email message dated October 26, 2000 from Attorney Brian Russell to all three co-inventors explaining his progress in revising the draft application.

12. Exhibit G denotes an email message dated November 6, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached revised application for co-inventor review.

13. Exhibit H denotes an email message dated November 6, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached revised application for co-inventor review.

14. Exhibit I denotes an email message dated November 8, 2000 from co-inventor Lei Yao to Attorney Brian Russell acknowledging receipt of revised applications for co-inventor review.

15. Exhibit J denotes an email message dated November 8, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached file related to the above-referenced application for co-inventor review.

14. Exhibit K denotes an email message dated November 21, 2000 from co-inventor Lei Yao to Attorney Paul Roberts reporting attached consolidated co-inventor comments for a final draft of at least the above-referenced application.

15. Exhibit L denotes an email message dated November 22, 2000 from Attorney Brian Russell to all three co-inventors reporting his incorporation of their comments into a final draft of the above-referenced application and requesting current address information for preparation of formal documents for all three co-inventors.

16. The above-referenced application was subsequently filed on November 28, 2000, as evidenced by the Updated Filing Receipt (Exhibit M).

17. Due diligence was exercised from prior to October 27, 2000 to the filing date of November 28, 2000 (Exhibits B - M).

18. We do not know and do not believe that our invention has been in public prior to our application, and we have never abandoned the invention.

19. All statements made herein are true of our own knowledge and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the patent.

Respectfully submitted,

______________________ Date — Dave McDysan

H Lee Thomas

______________________ Date — Howard Lee Thomas

______________________ Date — Lei Yao

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: David E. MCDYSAN et al.		Conf. No.:	7593
Application No.:	09/723,501	Examiner:	Gold, A.
Filed:	November 28, 2000	Group Art Unit:	2157
Customer No.:	25537		
Attorney Docket No.:	RIC00043		
Client Docket No.:	09710-1236		

For: EXTERNAL PROCESSOR FOR A DISTRIBUTED NETWORK ACCESS SYSTEM

Assistant Commissioner for Patents
Alexandria, VA 22313-1450

DECLARATION UNDER 37 CFR 1.131

Dear Sir:

We, Dave McDysan, Howard Lee Thomas, and Lei Yao, declare as follows:

1. We were employed by MCI, Inc., now an affiliate of Verizon Communications, Inc., assignee in interest for the subject matter of the above-referenced patent application, U.S. Application Serial Number 09/723,501, when the invention was conceived in this country and when the application was subsequently filed on November 28, 2000. In that capacity, we have personal knowledge of the facts and circumstances stated herein, except those statements which are made upon information and belief as set forth below.

2. We are joint inventors of the above-referenced patent application (Exhibit N).

3. It is our understanding that an Office Action mailed January 13, 2006 for the present application rejected claims 2-6, 9, 20-24, 27, 37, and 38 under 35 U.S.C. § 102(e) as anticipated by *Miles et al.* (U.S. 6,665,495) and rejected claims 7-8, 10-18, 25-26, 28-36 as obvious under 35 U.S.C. § 103(a) based, at least in part, on *Miles et al.*

4. We conceived our invention in this country long prior to October 27, 2000 (hereinafter the effective date), the effective filing date of U.S. Patent No. 6,665,495 entitled "Non-Blocking, Scalable Optical Router Architecture and Method for Routing Optical Traffic" to Miles et al.

5. Long prior to October 27, 2000, we prepared a description of our invention, a copy of which is attached hereto (Exhibit A). Although the dates of inventor signatures, headers, footers, and additional descriptive material has been redacted, we attest that the description was prepared long prior to the effective date of October 27, 2000.

6. Prior to October 27, 2000, and through November 28, 2000, we collaborated with Attorneys Brian Russell and Paul Roberts at least by telephone and email in their preparation of drafts of the above-referenced patent application, to review the drafts and suggest revisions, as evidenced at least by Exhibits B - L, in which page headers and footers, internal numbers, telephone numbers, email addresses, names of people copied on correspondence, and dates and times have been redacted.

7. Exhibit E denotes an email message dated August 31, 2000 from Attorney Brian Russell to co-inventor Lei Yao explaining that a draft application was almost complete for co-inventor review.

8. Exhibit D denotes an email message dated September 5, 2000 from co-inventor Lei Yao to Attorney Brian Russell acknowledging receipt of the email of Exhibit E.

9. Exhibit C denotes an email message dated September 5, 2000 from Attorney Brian Russell to co-inventor Lei Yao reporting an attached draft application for co-inventor review.

10. Exhibit B denotes an email message dated October 5, 2000 from co-inventor Lei Yao to Attorney Brian Russell reporting attached consolidated co-inventor comments on a draft application.

11. Exhibit F denotes an email message dated October 26, 2000 from Attorney Brian Russell to all three co-inventors explaining his progress in revising the draft application.

12. Exhibit G denotes an email message dated November 6, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached revised application for co-inventor review.

13. Exhibit H denotes an email message dated November 6, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached revised application for co-inventor review.

14. Exhibit I denotes an email message dated November 8, 2000 from co-inventor Lei Yao to Attorney Brian Russell acknowledging receipt of revised applications for co-inventor review.

15. Exhibit J denotes an email message dated November 8, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached file related to the above-referenced application for co-inventor review.

14. Exhibit K denotes an email message dated November 21, 2000 from co-inventor Lei Yao to Attorney Paul Roberts reporting attached consolidated co-inventor comments for a final draft of at least the above-referenced application.

15. Exhibit L denotes an email message dated November 22, 2000 from Attorney Brian Russell to all three co-inventors reporting his incorporation of their comments into a final draft of the above-referenced application and requesting current address information for preparation of formal documents for all three co-inventors.

16. The above-referenced application was subsequently filed on November 28, 2000, as evidenced by the Updated Filing Receipt (Exhibit M).

17. Due diligence was exercised from prior to October 27, 2000 to the filing date of November 28, 2000 (Exhibits B - M).

18. We do not know and do not believe that our invention has been in public prior to our application, and we have never abandoned the invention.

19. All statements made herein are true of our own knowledge and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the patent.

Respectfully submitted,

Date — Dave McDysan

Date — Howard Lee Thomas

03/07/2006
Date — Lei Yao

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	David E. MCDYSAN et al.	Conf. No.:	7593
Application No.:	09/723,501	Examiner:	Gold, A.
Filed:	November 28, 2000	Group Art Unit:	2157
Customer No.:	25537		
Attorney Docket No.:	RIC00043		
Client Docket No.:	09710-1236		

For: EXTERNAL PROCESSOR FOR A DISTRIBUTED NETWORK ACCESS SYSTEM

Assistant Commissioner for Patents
Alexandria, VA 22313-1450

DECLARATION UNDER 37 CFR 1.131

Dear Sir:

We, Dave McDysan, Howard Lee Thomas, and Lei Yao, declare as follows:

1. We were employed by MCI, Inc., now an affiliate of Verizon Communications, Inc., assignee in interest for the subject matter of the above-referenced patent application, U.S. Application Serial Number 09/723,501, when the invention was conceived in this country and when the application was subsequently filed on November 28, 2000. In that capacity, we have personal knowledge of the facts and circumstances stated herein, except those statements which are made upon information and belief as set forth below.

2. We are joint inventors of the above-referenced patent application (Exhibit N).

3. It is our understanding that an Office Action mailed January 13, 2006 for the present application rejected claims 2-6, 9, 20-24, 27, 37, and 38 under 35 U.S.C. § 102(e) as anticipated by *Miles et al.* (U.S. 6,665,495) and rejected claims 7-8, 10-18, 25-26, 28-36 as obvious under 35 U.S.C. § 103(a) based, at least in part, on *Miles et al.*

4. We conceived our invention in this country long prior to October 27, 2000 (hereinafter the effective date), the effective filing date of U.S. Patent No. 6,665,495 entitled "Non-Blocking, Scalable Optical Router Architecture and Method for Routing Optical Traffic" to Miles et al.

5. Long prior to October 27, 2000, we prepared a description of our invention, a copy of which is attached hereto (Exhibit A). Although the dates of inventor signatures, headers, footers, and additional descriptive material has been redacted, we attest that the description was prepared long prior to the effective date of October 27, 2000.

6. Prior to October 27, 2000, and through November 28, 2000, we collaborated with Attorneys Brian Russell and Paul Roberts at least by telephone and email in their preparation of drafts of the above-referenced patent application, to review the drafts and suggest revisions, as evidenced at least by Exhibits B - L, in which page headers and footers, internal numbers, telephone numbers, email addresses, names of people copied on correspondence, and dates and times have been redacted.

7. Exhibit E denotes an email message dated August 31, 2000 from Attorney Brian Russell to co-inventor Lei Yao explaining that a draft application was almost complete for co-inventor review.

8. Exhibit D denotes an email message dated September 5, 2000 from co-inventor Lei Yao to Attorney Brian Russell acknowledging receipt of the email of Exhibit E.

9. Exhibit C denotes an email message dated September 5, 2000 from Attorney Brian Russell to co-inventor Lei Yao reporting an attached draft application for co-inventor review.

10. Exhibit B denotes an email message dated October 5, 2000 from co-inventor Lei Yao to Attorney Brian Russell reporting attached consolidated co-inventor comments on a draft application.

11. Exhibit F denotes an email message dated October 26, 2000 from Attorney Brian Russell to all three co-inventors explaining his progress in revising the draft application.

12. Exhibit G denotes an email message dated November 6, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached revised application for co-inventor review.

13. Exhibit H denotes an email message dated November 6, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached revised application for co-inventor review.

14. Exhibit I denotes an email message dated November 8, 2000 from co-inventor Lei Yao to Attorney Brian Russell acknowledging receipt of revised applications for co-inventor review.

15. Exhibit J denotes an email message dated November 8, 2000 from Attorney Brian Russell to all three co-inventors reporting an attached file related to the above-referenced application for co-inventor review.

14. Exhibit K denotes an email message dated November 21, 2000 from co-inventor Lei Yao to Attorney Paul Roberts reporting attached consolidated co-inventor comments for a final draft of at least the above-referenced application.

15. Exhibit L denotes an email message dated November 22, 2000 from Attorney Brian Russell to all three co-inventors reporting his incorporation of their comments into a final draft of the above-referenced application and requesting current address information for preparation of formal documents for all three co-inventors.

16. The above-referenced application was subsequently filed on November 28, 2000, as evidenced by the Updated Filing Receipt (Exhibit M).

17. Due diligence was exercised from prior to October 27, 2000 to the filing date of November 28, 2000 (Exhibits B - M).

18. We do not know and do not believe that our invention has been in public prior to our application, and we have never abandoned the invention.

19. All statements made herein are true of our own knowledge and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the patent.

Respectfully submitted,

Dave McDysan

Date

March 9, 2006

Dave McDysan

Date

Howard Lee Thomas

Date

Lei Yao

[redacted] [redacted]

[redacted] Provide a short, descriptive title of the invention:
Distributed Programmable Access Device Network Supported by Separate Service Controllers

[redacted] When and under what circumstances was the invention first conceived (if you have any written evidence of this date, include copies):
The invention was born out of initiatives within the Company to provide customers with integrated access to all Company services and to provide customers with dynamic capabilities to adjust their services, either in type or quantity. The inventors [redacted] developed this invention while working on various projects directed toward pushing network intelligence and integrated access to the edge of the network and separating switching and routing from control functions throughout the network.

[redacted] What is the date of the first sketch or drawing of the invention:
[redacted]

[redacted] What is the date of the first written description of the invention:
[redacted]

[redacted] What is the date of the first test of or operation of the invention:
[redacted]

[redacted] List all contributors (use other pages if necessary) to this conception of the invention and indicate the contributor's company if not an MCI WorldCom employee (also identify one person as a primary contact with an "X" next to the name):

X Printed Name: ___McDysan_____ David_____ E._____
Last name First Middle initial

***Please record your name correctly: Last Name, First Name, Middle Initial; DO NOT USE NICKNAMES, etc.**

Phone#: [redacted] (h) _____ Dept/Loc: [redacted] E-MailID: [redacted]

Current Address: [redacted]
City State Zip code

Country: __USA____ Citizenship: ___USA____ Job Title: [redacted]

Job assignment at invention conception: [redacted]

Printed Name: ___Thomas_____ H._____ Lee_____
Last name First Middle initial

Phone#: [redacted] Dept/Loc: [redacted] E-MailID: [redacted]

Current Address: [redacted]
Street City State Zip code

Country: ___USA____ Citizenship: ___USA____ Job Title: [redacted]

Job assignment at invention conception: [redacted]

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E McDysan		Print Name H Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted] [redacted]

Printed Name: ___Yao________________________Lei____________________________________
Last name First Middle initial

Phone#[redacted] (h) ____________ Dept/Loc: [redacted]___ E-MailID: [redacted]______

Current Address: _[redacted]______ [redacted]________ [redacted]________
Street City State Zip code

Country: ___USA_________ Citizenship: ___China______ Job Title: ___[redacted]______________

Job assignment at invention conception: _________[redacted]________________________

[redacted] [redacted]

[redacted]

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
[signature]	[redacted]	H Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted] [redacted]

[redacted] Describe the invention using the following format. Use as many pages as necessary. **Mark each additional page "MCI WorldCom Confidential."**

1. Discuss the problems which the item is designed to solve. Refer to any prior devices of a similar nature with which you may be familiar.

   A. Today's routers implement the routing, forwarding, policy, policing, marking, and admission control functions in a monolithic, proprietary manner. A few routers have limited implementation of external policy control. The services that a provider can offer are limited by the control software implemented by a particular router/switch vendor. If a service provider has routers from multiple vendors in a network, the proprietary services will not inter-operate. Consequently, the service provider is not able to purchase router/switches from one vendor and purchase policy-based service control from another vendor. Furthermore, a service provider cannot offer its network as a platform for a wholesale provider to offer value-added services utilizing the existing base network capabilities.

   B. The implementation of the multiple functions listed above in a monolithic router presents a significant scalability challenge for vendors in response to the phenomenal growth of Internet traffic. The current design approach by the industry separates the problem into core and access routers. Access routers perform the most complex functions and perform operations that simplify the tasks required of core routers. However, the monolithic design of access routers presents a limit for scalability of the Internet. Evidence of this fact is that the access router software image size is increasing.

   C. Another problem brought on by the rapid growth of Internet traffic is the need to dynamically provision, configure, and/or reallocate access capacity to IP-based services. Access capacity is often limited and a major cost component of modern networks. Therefore, it is subject to congestion and has a strong need for admission control and different levels of quality. Also, access products are not capable of handling a wide variety of traffic types while being able to enforce policy controls (provider-initiated or customer-initiated) or dynamic requests for capacity.

   D. Today's routers cannot distinguish between higher layer message types and forward the higher layer messages according to service/policy parameters. Today's routers do not use a combination of protocol type, source IP address (SA), destination IP address (DA), type of service (TOS) or differentiated service code-point (DSCP), source port number (SP) and destination port number (DP) to distinguish different message types. In fact, most routers use only the DA to make the forwarding decision. Some newer routers use only DA plus TOS/DSCP.

   E. Today's access routers have a concept of one controller providing all services for all message types. This results in a single complex router, which is difficult to add new services or modify existing services. This monolithic design limits flexibility and extensibility and increases cost. Evidence of this fact is that the time to market for new features and functions are delayed. For example, In today's network, if a service provider's external policy server sends COPS messages to an access router, the service provider must ask the vendor to develop a COPS interface on the router.

   F. Today's routers have relatively weak security control of their configuration information. For example, a command line interface is invoked by a simple userid password exchange in the clear when initiating over a telnet session.

   G. Desktop computing applications provide customers with the means to utilize many different services while each service requires different (quality of) service requirements. Today's networks do a poor job of identifying which traffic is associated with which service. Therefore, applications vie for whatever network resources can be obtained in a first-come, first-served fashion.

   H. Traffic patterns are shifting from the traditional telecommunications model where the community of interest was primarily local to one where the community of interest is distance independent.

   I. Today's network is not able to measure or monitor the statistics of layer-2 and layer-3 traffic types and take advantage of dynamic network capabilities to add network resources to support customer Service Level Agreements (SLAs).

   The invention is similar to FAST with respect to the separation of signaling and switching and interaction with policy servers. This disclosure extends these concepts to IP connectionless protocols as well as higher layer session and application layer protocols.

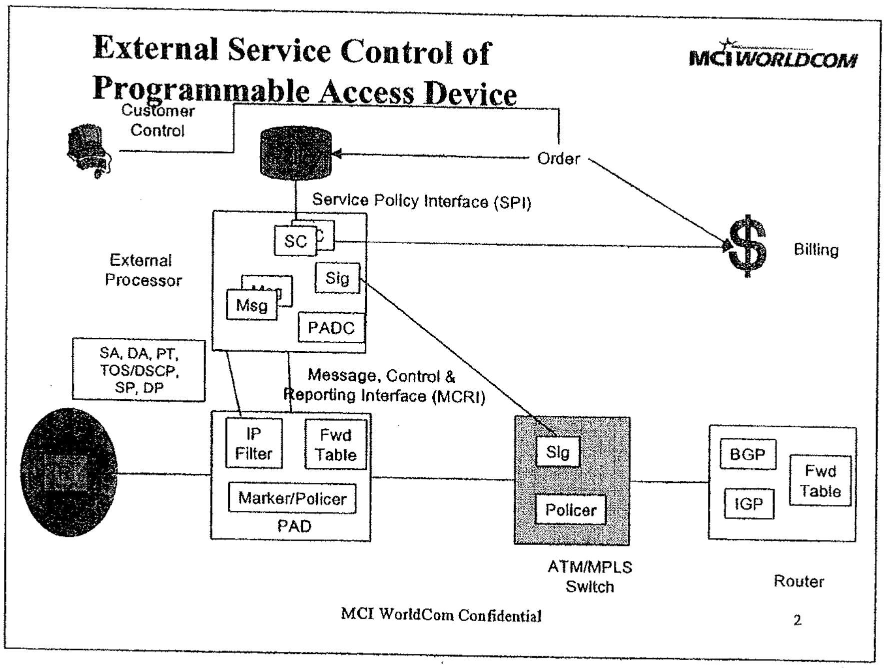
2. Describe how the invention qualifies as a solution to the problem, and state the advantage of the item over presently known devices, systems or processes.

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted]

A. The invention decomposes the traditional router into a Programmable Access Network with distributed service control (PANDSC) and hardware/software Service Controllers (SC) executing on external processors as shown in Figure 1. The SCs interface to the PAD using a Message Control and Reporting Interface (MCRI). The PAD uses the MCRI to pass service-specific messages to/from the corresponding service controller software/hardware executing on an external processor. The PAD uses fields in the network, transport and application layer headers to identify a particular traffic flow and determine which messages are passed to a specific service controller. One or more service controllers may remotely control a single PAD; however, only one SC would control a particular traffic flow. Additionally, the PAD can report on events of statistics of received traffic according to parameter ranges and intervals defined by the SC. The combination of the PAD functions of service-specific message forwarding, remote control, and reporting enables the implementation of the service controllers by different vendors than those implementing the PAD.



B. The invention achieves superior scalability when compared with traditional routers since it separates out the functions performed by a router into three platforms. Routing is still done in the router as shown on the right-hand side of Figure 1. However, the functions of filtering, message forwarding, policing, and marking are placed in the PAD. Finally, the message interpretation, signaling, admission control, and policy invocation is implemented in SCs on external processors.

C. The Programmable Access Device and SC enable customer applications to reserve bandwidth, perform admission control, and prioritize traffic streams based upon available capacity and policy controls. These policy controls may be initiated by the provider or the customer organization. The capability for customer applications to interact with service provider network resources provides the customer the ability to dynamically provision services as well as provide applications the required quality of service guarantees. If the PAD is located at the extreme edge of the network, then the external processor can signal for access capacity. This network-based provisioning invoked by policy control replaces time-consuming and error-prone OSS provisioning.

D. The IP filter in the PAD provides the ability to identify higher layer message types (network, transport and application layers) and forward those messages from/to the external processor based on the parameters configured by message processor. The IP filter will have the ability to use a combination of protocol type, SA, DA, TOS or DSCP, SP, DP and other fields to distinguish different message types.

E. Each service controller executing on the external processor supports a specific type of service. (Each service controller may be based on a generic controller with service-specific APIs.) The invention allows implementation of new services by the introduction of new SCs (or modification of existing SCs) without requiring changes to the PAD. Multiple service controllers provides the ability to add new services or modify existing services by the addition or replacement of service controllers rather than requiring all services to be disrupted during upgrades.

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted] [redacted]

SCs can be installed on multiple external processors. Additional external processors are easily added according to service requirements, which results in the good scalability.

F. The external processors provide added security against theft of services and attacks. The external processors may be maintained in a secure environment while leaving the forwarding functions of the PAD in a less-secure environment. In addition to being physically separate from the PAD, security software and/or hardware on the external processor may be implemented. TCP sessions to configure the PAD from the IP addresses other than its master external processors would be denied by the IP Filter.

G. Since the PAD intercepts network, transport and application level messages, it enables the identification of applications and users, and sets up an appropriate priority or provides the desired bandwidth to the data flows of user applications. For example, RSVP together with Microsoft subnet bandwidth manager (SBM) provides an application with guaranteed bandwidth and priority end-to end across the local and wide area networks.

H. As Internet traffic patterns change to be well-distributed around the globe, the ability to apply service and policy at the access separately from routing on a regional basis provides a more scalable design for forwarding traffic toward the distant destination.

I. The usage monitor in PAD is able to track the statistics of different layer-2 and layer-3 traffic types. When the volume of traffic for a specific type across a threshold, this event is reported to SC. The Signaling Processor within the External Processor works with the SC to ensure that active SLAs are maintained throughout the network. This coupling of the policy accessed by the SC and the dynamic SLA support in the network provides a more flexible solution that is available with today's TDM approach to SLAs.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

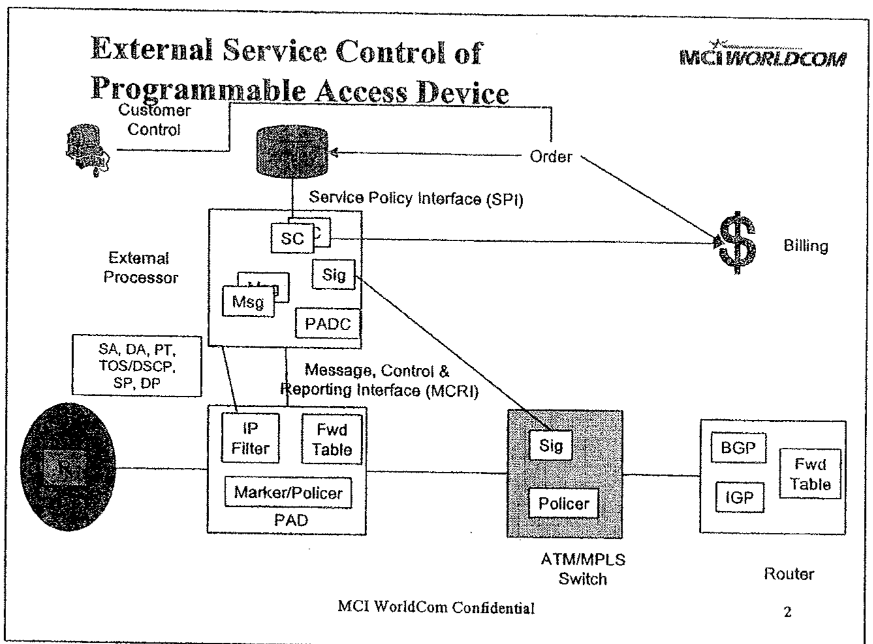
Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted]

Figure A.1 shows the components of the Access system implementing the PAD and SC concept. The Access system includes an External Processor, a PAD and a Policy Server. The SPI (Service Policy Interface) is the interface between Policy Server and SCs. MCRI (Message Control and Reporting Interface) is the interface between SCs and PAD. Detailed descriptions of these components and interfaces are contained in this section.

The External Processor is a general purpose computer and/or a special purpose hardware to providing environment for one or multiple SCs and interface device drivers. A service controller can be implemented either by hardware or by software. A service controller is able to interpret service-specific messages and invoke the appropriate policy control and network signaling procedure. The service controller configures the PAD using MCRI according to the policy decisions received from the Policy Server via the SPI. Separation of the SC processing from the forwarding performed in the PAD allows allocation of external processing resources to SC functions as necessary without degrading the forwarding performance of the PAD. In fact, SCs can be allocated to external processors and PADs in an arbitrary manner in response to access traffic patterns. [redacted]



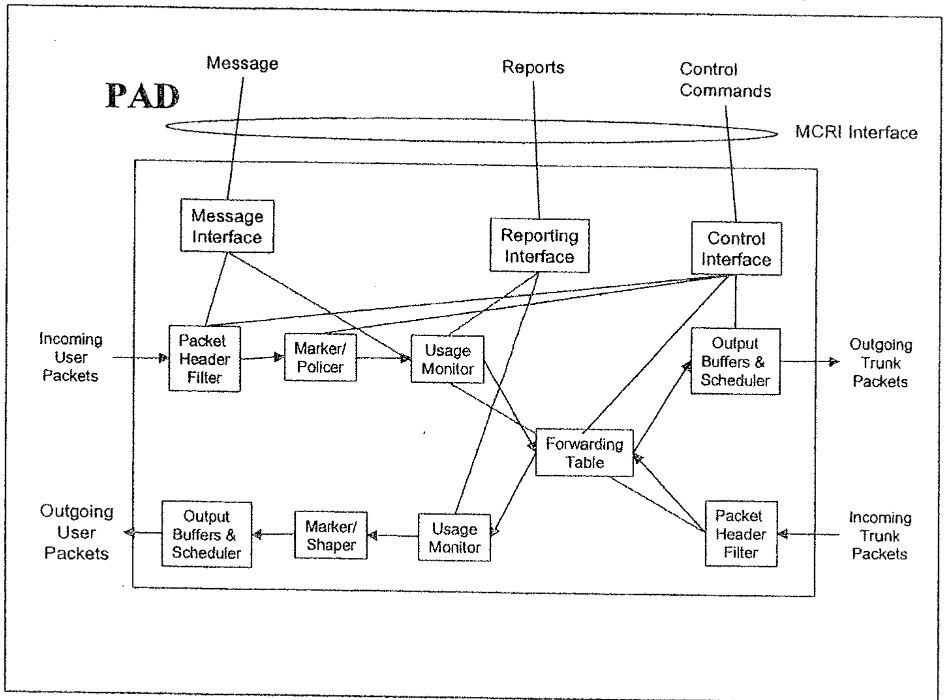
(Figure A.1 External Service Control and PAD)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted] [redacted]

A.2 Programmable Access Device (PAD)



(Figure A.2 PAD)

Figure A.2 shows the detailed components of the PAD. The PAD is a programmable access device with generic forwarding, marking, policing and IP filter functions. [redacted]

The Packet Header Filter operates on the DA, SA, TOS, SP, DP and other fields of a packet received from a user device and is configured by the control interface. It either directs a packet to a specific marker/policer, or else redirects the packet to the message interface. The message interface may also inject a packet into the Packet Header Filter.

The policer applies one or more token or leaky bucket algorithms to the stream of received packets to determine conformance to traffic parameters established by the control interface. The results of the policing function can be discard of nonconforming packets, marking of nonconforming packets, or counting of nonconforming packets.

The marker function sets the bits in the DiffServ/TOS byte, and/or the 3-bit MPLS experimental field, and/or the 20-bit MPLS label field, and/or other fields for a specific flow as configured by the control interface.

The Usage monitor tracks the statistics of different layer-2 and layer-3 traffic types. Thresholds and other criteria can be set up to invoke a reporting event. The reporting messages sent to the SC may summarize the usage information for a customer, report the occurrence of a high-priority traffic flow or warn the large volume of out-of-band traffic etc.

Output buffers can be a single large buffer or distributed multiple buffers. A percentage of the total buffer or a fixed amount of buffer can be assigned to a class of traffic or a traffic flow classified by DA, SA, TOS, PT, SP and DP. Packet scheduler applies Weighted Round robin and other algorithms to support statistical multiplexing. The combination of the buffering mechanism and scheduling mechanism can put a limit on the queuing delay to transmit a packet over the PAD.

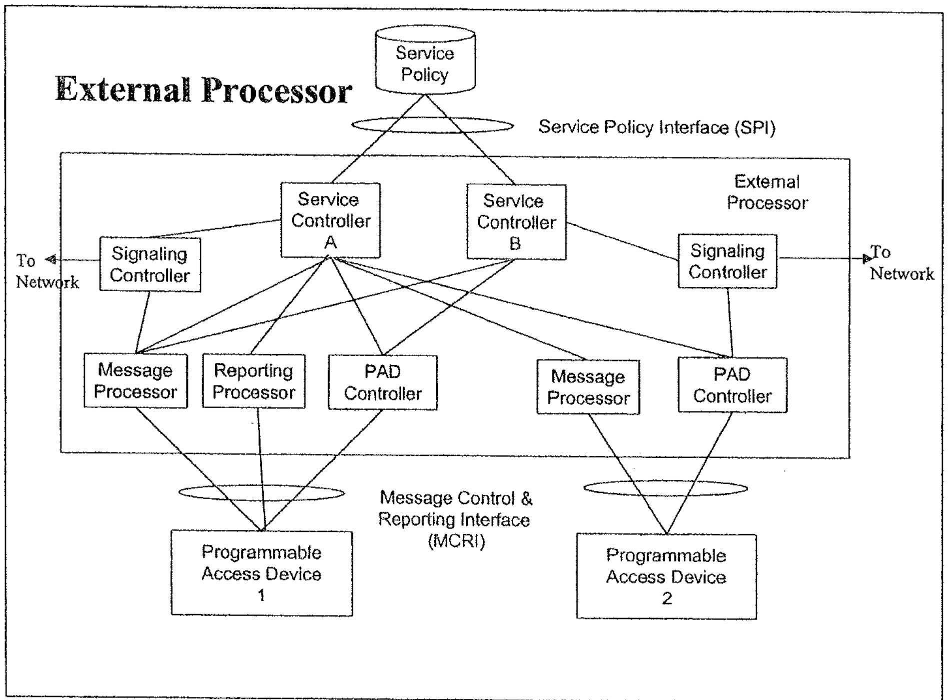
The Shaper discards the nonconforming packets, sends marked packets to appropriate queues, and controls the delay jitter of a flow.

Forwarding table keeps entries for each forwarding path. A forwarding path is represented by the packet flow attributes, i.e. DA, SA, TOS, PT, SP, DP, the incoming port and the corresponding output port.

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

A.3 External Processor



(Figure A.3 External Processor)

Figure A.3 illustrates the logical elements within the External Processor. The External Processor is composed of several control and process functions that are utilized by policy servers and PADs to determine and affect the appropriate processing of packets and messages to and from customer applications.

PADs send messages, report information and control commands to the External Processor through the Message Control & Reporting Interface (MCRI). The Message Processor, Reporting Processor and PAD Controller utilize the MCRI.

The Reporting Processor and Message Processor parse messages from PADs and notify the SC of the semantics of the messages. [redacted] The Report Processor is able to configure the reporting functions of the PAD including the type of reporting message, the content in the reporting message, whether to pass or not pass report information, etc. The Message Processor is able to configure the IP filter to pass or not pass specific messages based on SA, DA, PT, SP, DP and/or other fields.

The PAD controller configures and manages the PAD. The PAD Controller operates on the PAD Forwarding table, IP filter, Usage Monitor, Marker/Policer/Shaper, Buffer and Scheduler by commands or scripts.

The Signaling Controller supports signaling protocols (e.g. RSVP, LDP, PNNI, FR UNI, ATM UNI, etc.) to set-up or tear down a VC or LSP across the network. The VC or LSP may have QoS specification with it.

The Service Controller (SC) is the main control module for each service. It translates the messages from the Message Processor and Reporting Processor into appropriate policy queries and sends them to the PDP. It launches VC or LSP setups across the network through the Signaling Controller. It configures forwarding table, IP filter, Marker/Policer, Shaper, buffer and scheduler on a PAD by the PAD controller. All these working together delivers the desired service for the customer traffic. [redacted]. Each PAD has at least a primary and secondary SC. If a PAD loses contact with the primary SC contact will be initiated with the secondary SC. The PAD will report state information to the secondary SC. [redacted]

To reduce the number of messages passed between a SC and the PDP, SCs [redacted] cache the frequently used policy lookups in its policy caches. For an incoming policy query, a SC looks up its policy caches first before it sends the query to the PDP. When a SC directly queries the PDP for a new service request, the SC may also request the PDP to dump all the related policy information from the policy database to its policy caches. Caching enables subsequent policy queries to utilize information that has already been retrieved recently from the policy server and reduce the message traffic between the SC and PDP. However there is a tradeoff between the number of direct policy queries and the cache refresh frequency and the amount of policy information downloaded from the PDP at each refresh. The objective would be to cache the

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[signature] [redacted]	[signature] [redacted]	[signature] [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted] policies for IP services requiring intensive policy queries, such as SIP calls. There would be no need to cache the policy lookups for a TCP session that issues only one policy query in its lifetime.

The PDP within a policy database interacts with a SC by utilizing the Service Policy Interface (SPI). With the SPI, a SC is able to use COPS, LDAP and other policy query protocols to query the PDP within the policy database. The policy database resides on a policy server which would be an external processor resident on hardware separate from the External Controller and placed in different locations within the network. The SC sends policy requests to the PDP. The PDP returns the policy decisions for each request. The policy decision can be "approve", "reject" or configuration parameters for the SC and PAD. The PDP maintains usage information used by policy decision. [redacted]

With open SPI and MCRI, the carrier administrator should have the full control of the SCs and programmable access devices by writing scripts or configuring parameters. Customers could also be granted limited control over the SCs and PADs in support of self-provisioning.

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted]

A.4 Interfaces

A.4.1 Service Policy Interface (SPI)

PDP to SC

- Set Inactivity Timer
- Approve the transaction
- Reject the transaction with a cause indication
- Return parameters in response of request
- Dump the policy lookups into SC policy caches

SC to PDP

- Translate Signaling Messages into appropriate Policy Queries, e.g. RSVP -> COPS (RSVP), SIP-> COPS (SIP)
- Query Policy Requirements
- Set the flag for caching of Policy lookups
- Translate Policy Decisions into appropriate control commands

A.4.2 Message, Control and Reporting Interface (MCRI)

PAD to External Processor

- Message Passing
  - Pass based upon SA, DA, PT, SP, DP, and/or other fields such as TCP Flags (SYN, ACK, RST, FIN, ...)
- Reporting
  - TCP Retransmit Threshold Crossed
  - Inactivity Timer Expired
  - Activity Detected
  - Keepalive/Heartbeat Exchange
  - State synchronization in event of SC switchover
  - Traffic Threshold Crossed
  - Usage Statistics
- Control
  - Acknowledgement of Command
  - Command Failure indication

External Processor to PAD

- Message Passing
  - Inject packets into the user of trunk side interface
  - Set pass/no pass flag based upon SA, DA, PT, SP, DP, and/or other fields
- Control
  - Configure IP Filter
  - Configure Marking
  - Configure Policing
  - Configure Output buffers & Scheduler
  - Configure Shaper
  - Drop multicast packets from a source
  - Admit/Deny Source Routing Option
  - Set TCP Retransmit Reporting Threshold
  - Set Inactivity Timer
  - Set Activity Timer and Level
  - Configure Forwarding Table
  - Set Traffic Reporting Threshold
  - Allocate Resource (Bandwidth, Queue & CPU time) to a customer, a flow, a route or a multicast tree
  - Set Reporting Flags (True/False)
  - Set SVC, PVC or LSP

A.4.3 PAD-SC Switchover Operation

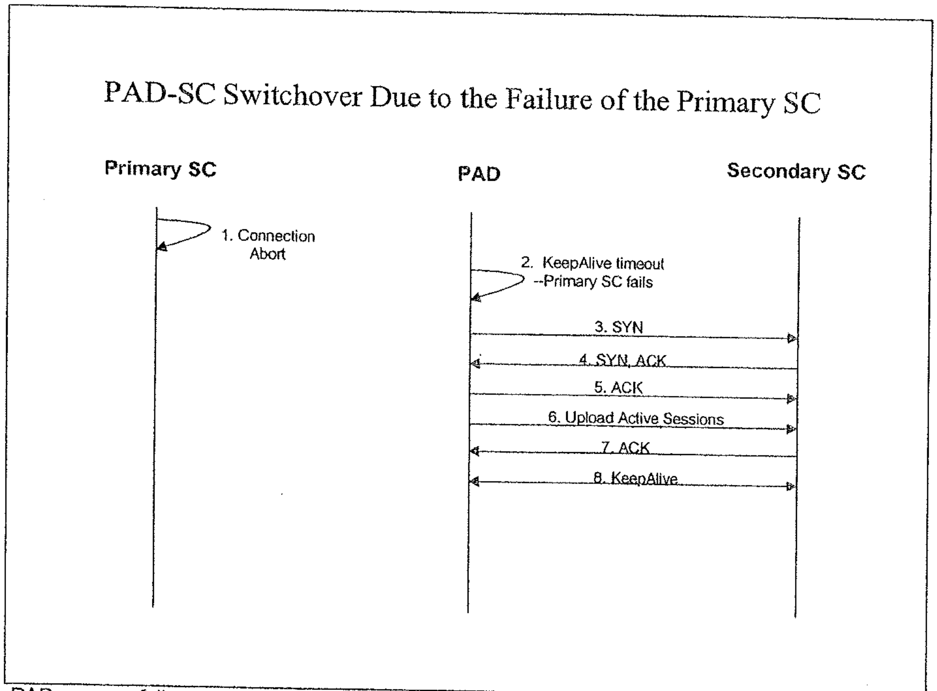
To prevent the interruption of the service, the PAD will switch to a backup SC in the event of a fault in the primary SC or the loss of connectivity to the primary SC. The PAD uses a reliable communication protocol (e.g. TCP session) to exchange information with SCs. The KeepAlive message is exchanged between the PAD and a SC periodically to keep the TCP session active. When the KeepAlive message timeouts, the PAD detects the failure of the SC. The PAD starts setting up a new TCP session with the secondary SC. If the PAD could not connect with the

Inventor Signature / Date	Inventor Signature / Date	Inventor Signature / Date
David E McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted]

secondary SC, the PAD would stop accepting new sessions and keep the state and the service for all the active sessions. After the TCP session between the PAD and the secondary SC is established, the PAD starts uploading the state information of all the active sessions controlled by the failed SC to the secondary SC. The PAD is required to keep the state machine for each active session. (See Figure A.4 The PAD successfully switches from the primary SC to the secondary SC after detecting the failure of the primary SC)



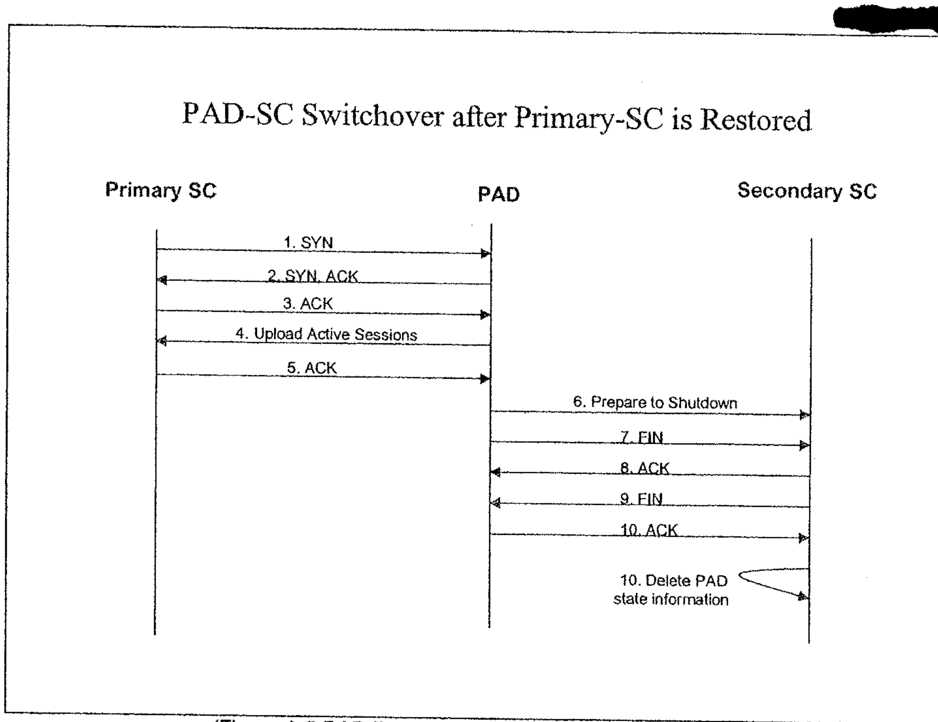
(Figure A.4 The PAD successfully switches from the primary SC to the secondary SC after detecting the failure of the primary SC)

The communication between the PAD and secondary SC may remain in a non-revertible mode, or may revert to the primary SC in a revertible mode to maintain load balancing of SC processing across the distributed PADs. Reversion to the primary SC may be accomplished with no service interruption as follows. When the primary SC begins working again, it sends TCP session set up message to the PAD. The PAD handshakes with the SC and recognizes that it is the primary SC. The PAD uploads all the active sessions to the primary SC. After the uploading is successfully completed, the PAD notifies the secondary SC that the primary SC is up and closes its TCP connection with the secondary SC. When the secondary SC gets the notice from the PAD that the primary SC is up, it closes the TCP connection with the PAD and deletes all the related state information. (See Figure A.5)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted]



(Figure A.5 PAD Restores Connection with Primary SC)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted] [redacted]

A.5 Examples

Several examples are provided below to illustrate how various network activities may be supported by the components of the proposed invention. Generic space-time drawings are used to illustrate the sequence of messages as they are passed between the various components of the PAD, SC and network. The following terms are used frequently in the space-time drawings:

Customer Site- Represents the point at which a device or application (typically at an end-user location) where service is desired. The customer application may be requesting, for example, network resources (e.g. RSVP) or to participate in a private broadcast (e.g. multicast).

PAD- The Programmable Access Device as described is section A.2.

PDP- The Policy Decision Point is a logical point that resides within the policy server. Messages to and from the PDP are carried by the Service Policy Interface as described in sections A.3 and A.4.1.

Network- The network line in the drawings represents routers or switches within the service provider network that would that send a message or packet to an egress point or corresponding system at another access point on the network. The far end network system would process the request or packet being sent by the Customer Site or PAD.

The following examples are provided in the sections that follow:

Network-Level Signaling Example
- RSVP Signaling Example

Connection-Oriented Transport Examples Using TCP Sessions
- TCP State Machine on the PAD
- TCP Session Establishment
- TCP Session Close
- TCP Session Unauthorized
- TCP Session Timeout
- TCP Session Abrupt Close

Connectionless Transport Examples Using UDP Reporting Function
- UDP Reporting Successful
- UDP Reporting Unauthorized
- UDP Reporting Timeout

Application-Level Examples Using SIP Signaling
- SIP Call Establishment
- SIP Call Termination
- SIP Call Timeout
- SIP Call Negotiation

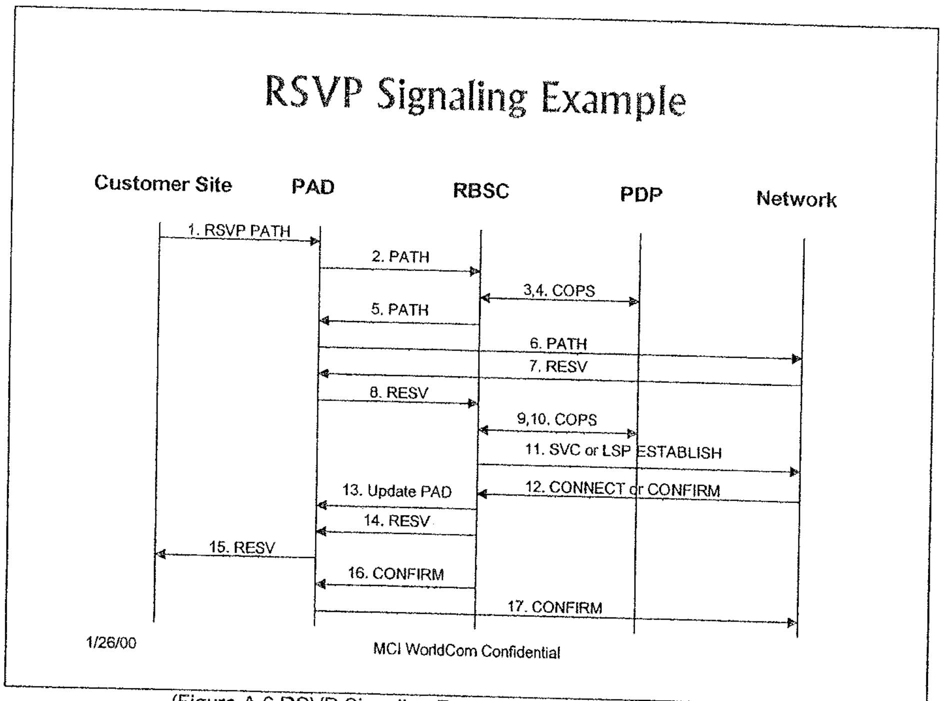
IP Multicast Examples
- Authorized Registration of a New Multicast Group
- Unauthorized Registration of a New Multicast Group
- Authorized Membership Query
- Unauthorized Membership Query
- Authorized Sending of Multicast Packets
- Unauthorized Sending of Multicast Packets
- Receiving Authorized Multicast Packets
- Receiving Unauthorized Multicast Packets

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

A.5.1 Network-level Signaling Example

In the example shown in Figure A.6, the customer application initiates an RSVP PATH message (1). The PAD forwards the PATH (2) message to the SC, which is called a Reserved Bandwidth Service Controller (RBSC) in this example. The RBSC queries the PDP (3). The PDP approves the RBS to the customer (4). The RBSC returns PATH (5) to PAD. PAD sends the PATH (6) message downstream to the other end of the network. The receiver responds by a reservation (RESV) message (7). The PAD passes the RESV (8) to the RBSC, which invokes another policy query (9). The PDP approves and records the bandwidth requirements by the RESV (10). (Here we assume that the PDP keeps track of the allocated bandwidth for a customer. The occupied bandwidth is compared with the committed bandwidth to a customer for policy-based admission decision.) The RBSC then kicks off either the ATM signaling or the MPLS signaling to set up a SVC or a LSP (11). After the connection is confirmed (12), the RBSC configures the PAD's IP filter and forwarding table to transmit packets of this flow over the established SVC or LSP (13). The RBSC in turn returns RESV (14) to the PAD. The PAD sends the RESV (15) upstream to the sender application. The RBSC also sends the CONFIRM downstream to the receiver (17) to finish the handshake for setting the SVC or the LSP. In this example, the IP filter in PAD captures RSVP messages according to its protocol type (PT=46).



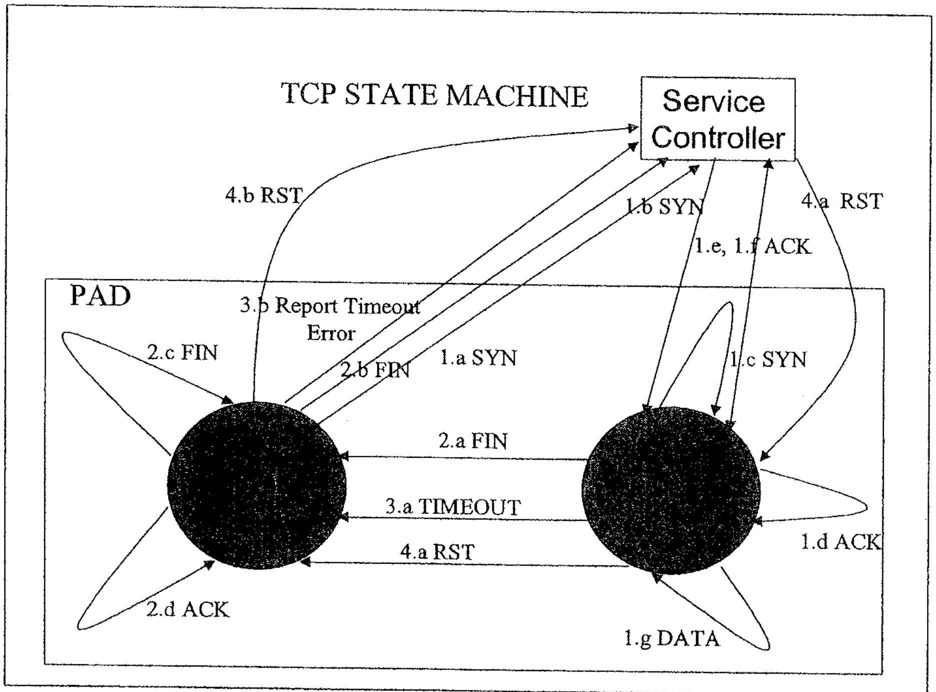
(Figure A.6 RSVP Signaling Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
[illegible]	[redacted]	[illegible]	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

A.5.2 Connection-oriented transport examples using TCP sessions:

- TCP State Machine on the PAD



(Figure A.7 TCP State Machine)

The TCP state machine on the PAD has two states: idle and active. The state transition is described below:

IDLE -> ACTIVE

1. When the state machine is in the idle state (non-existing TCP session), it passes and only passes the first SYN message received from the user to the SC (1.a). The SC queries the policy server for policy decisions for this TCP session after it receives the SYN message from the PAD. If the TCP session is approved, the SC returns the SYN message back to the PAD (1.b). The PAD changes the state machine to the active state and forwards the SYN message to the receiver to complete the three-way handshake (1.c, 1.d). The PAD passes the ACK message representing the success of the handshake to the SC (1.e). The SC knows the TCP session is open and adds the TCP session into its active session table. The SC updates the PAD with an inactive timer and other related parameters of this TCP session and then sends the ACK back to the PAD (1.f). The TCP session is ready for data transmission (1.g).

ACTIVE->IDLE

2. When the PAD receives a FIN message from the either side of a TCP connection for an active TCP session, it resets the TCP state machine to be idle (2.a). The PAD passes the FIN message to the SC (2.b). The SC learns that the TCP connection is inactive and deletes the TCP session from its active session table. The PAD forwards the FIN message to its destination to complete the three-way handshake for closing the TCP connection (2.c, 2.d). The PAD deletes the state machine of the TCP session.
3. When the inactive timer on the PAD for an active TCP session expires, the PAD resets the TCP session to be idle (3.a). The PAD reports the timeout error to the SC (3.b). The SC deletes the TCP session form its active session table and updates the PAD. The PAD deletes the state machine of the TCP session.
4. When the PAD receives a RST segment from either side of a TCP connection, it knows that an abrupt close is requested and resets the TCP session to be idle (3.a). The PAD reports the timeout error to the SC (3.b). The SC deletes the TCP session from its active session table and updates the PAD. The PAD deletes the state machine of the TCP session.

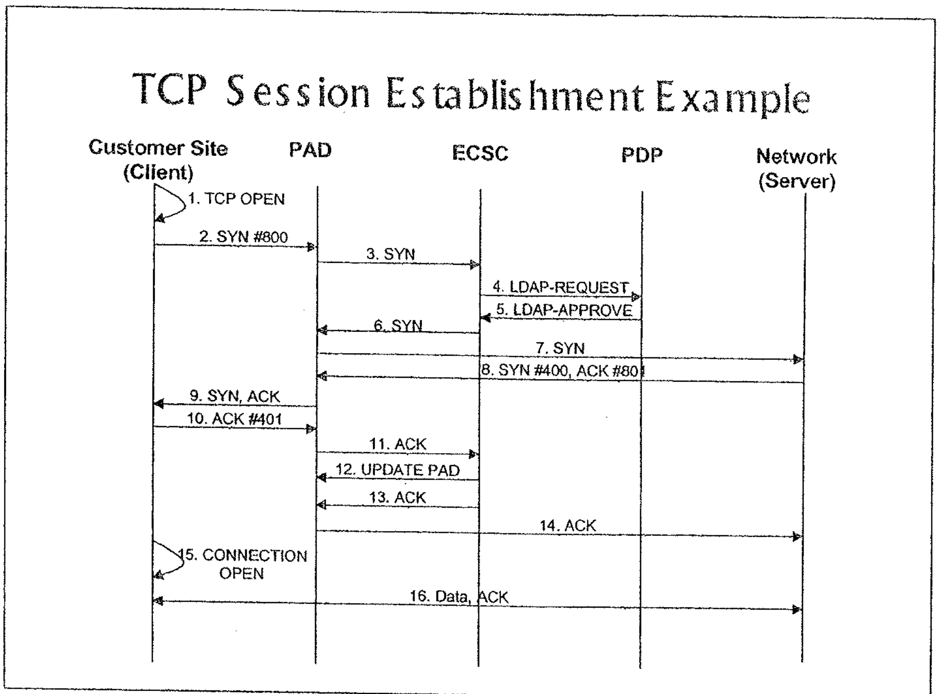
Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[redacted]	[redacted]	[redacted]
Print Name David E. McDysan	Print Name H Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted]

- TCP Session Establishment

  SCs configure the PAD to pass TCP SYN messages for non-existing TCP sessions to them. In the example shown in Figure A.8, The client application issues an OPEN (1) command that tells TCP that it wants to open a connection to a server at a given port and IP address. The client TCP picks an initial sequence number (800 in this example). The client TCP sends a synchronize segment (SYN) carrying this sequence number (2). When the SYN arrives, the PAD detects that it is a mission-critical e-commerce TCP session based on the destination IP address and port number (PT=6, PORT=80). The PAD passes the SYN to the e-commerce service controller (ECSC) (3). The ECSC asks for the policy and admission control from the PDP (4) using LDAP or some other policy query protocol. The PDP approves the TCP session (5). The ECSC sends the SYN back to the PAD (6). When the PAD receives the SYN from the ECSC, it spawns a new TCP state machine and sets it to an active state (7). The PAD sends the SYN downstream to the server (7). When the SYN arrives, the server TCP picks its initial sequence number (400 in this case). The server TCP sends a SYN segment containing initial sequence number 400 and an ACK of 801(8), meaning that the first data byte sent by the client should be numbered 801. The SYN/ACK message is sent back to the client (9). When the client TCP receives the server's SYN/ACK message, the client TCP returns an ACK of 401 (10), which means that the first data byte sent by the server should be numbered 401. The PAD passes the ACK to the ECSC (11). The ECSC learns that the three-way handshake is successful and the TCP session is open. The ECSC adds the TCP session into its active session table and configures the PAD (12) with the number of retransmissions and the inactive timer. The ECSC also sets the marker to mark the packets belonging to this TCP session as high priority. (For some applications, such as the training applications that will only allow the teacher to disconnect the TCP sessions, the SC configures the IP Filter to ignore the client FIN.) The ECSC then returns the ACK segment to the PAD (13). The PAD sends the ACK to the destination server (14). The client TCP notifies its upper layer application that the connection is open (15). The client and the server start exchanging data in the TCP session (16).

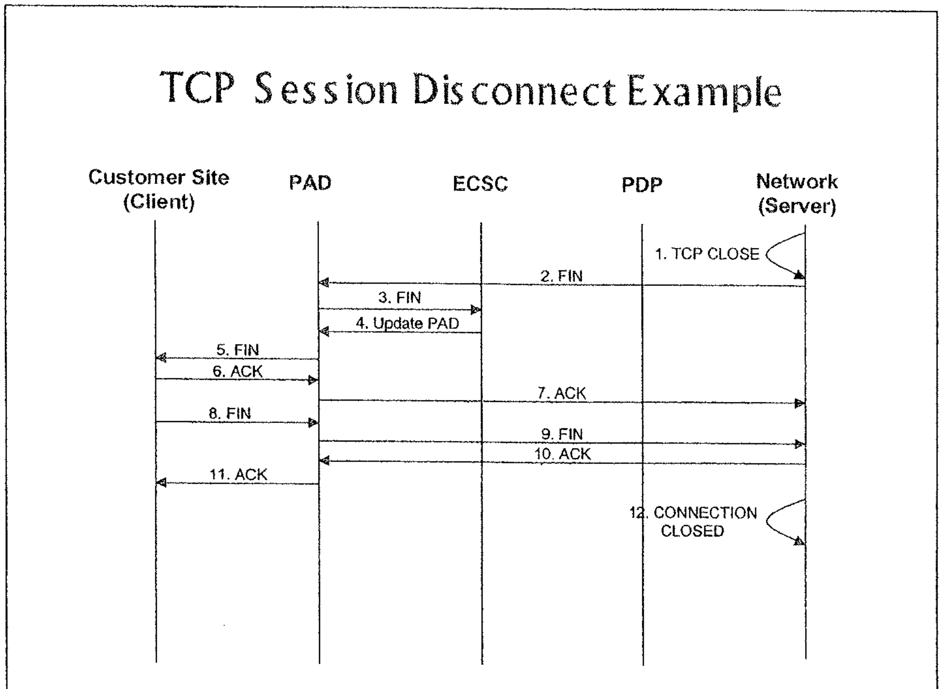


(Figure A.8 TCP Session Establishment Example)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

[redacted] [redacted]

- TCP Session Close
  Either side of a TCP connection can launch a close. The server initiates the close in the example shown in Figure A.9. The server application has finished its work and tells TCP to close the connection (1). The server TCP sends a FIN segment (2), informing the partner that it will send no more data. The PAD resets the state machine of the TCP connection to be idle and passes the FIN segment to the ECSC (3). The ECSC deletes the TCP session from its active session table and configures the PAD to stop marking packets for this TCP session (4). The PAD forwards the FIN segment to the client (5). The client TCP acknowledges receipt of the FIN segment (6, 7). The client TCP notifies its application that the client wishes to close. The client application tells its TCP to close. The client TCP sends a FIN message to the server TCP (8,9). The server TCP receives the client's FIN and responds with an ACK to the client (10). The PAD knows the three-way handshake for closing the TCP session is successful and deletes the state machine of this TCP session. The PAD then forwards the ACK to the client (11). The server TCP notifies its application that the connection is closed (13).



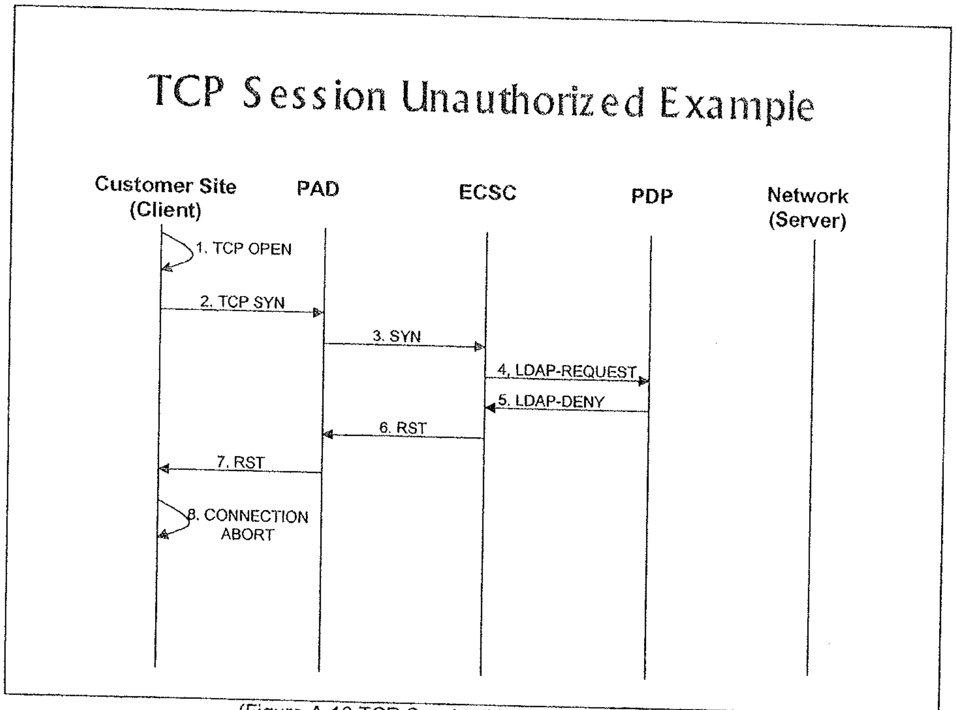
(Figure A.9 TCP Session Close Example)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

- TCP Session Unauthorized

In the example shown in Figure A.10, the client application issues an OPEN (1) command that tells TCP that it wants to open a connection to a server at a given port and IP address. The client TCP picks an initial sequence number. The client TCP sends a synchronize segment (SYN) carrying this sequence number (2). When the SYN segment arrives, the PAD detects that it is a mission-critical e-commerce TCP session based on the destination IP address and port number (PT=6, PORT=80). The PAD passes the SYN segment to the ECSC (3). The ECSC asks for the policy and admission control from the PDP (4) by LDAP. The PDP denies the TCP session either because there is not enough resources in the network or because the client has not ordered the e-commerce service (5). The ECSC in turn issues a reset segment to the PAD (6). The PAD sends the RST segment upstream to the client TCP (7). When the client TCP receives the RST, the client TCP aborts the session. (Note: Since the PAD does not receive a SYN segment from the ECSC, no state machine has been created for the TCP session in this example.)

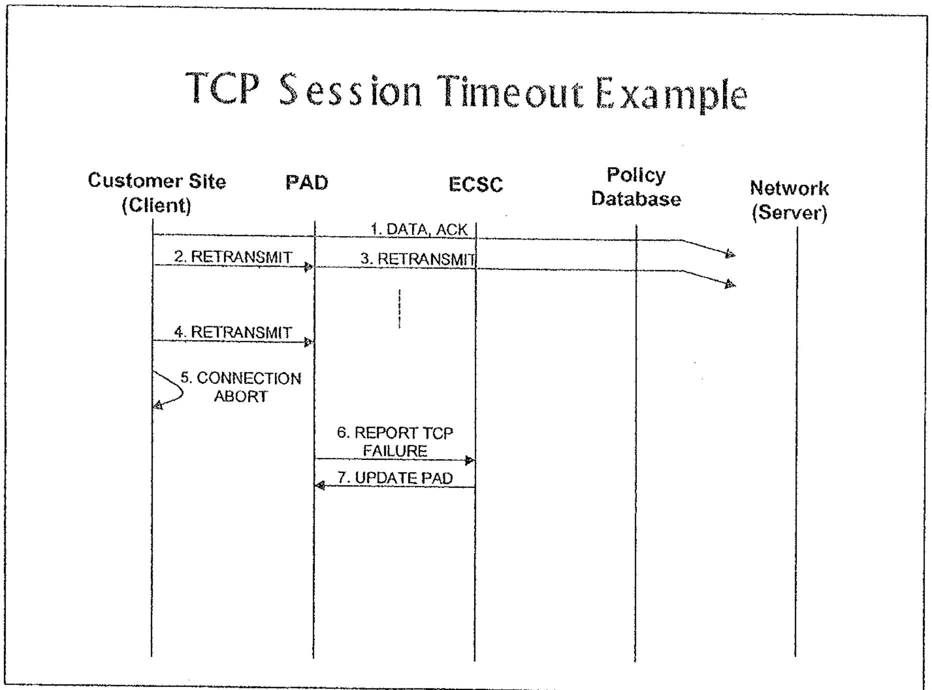


(Figure A.10 TCP Session Unauthorized Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	[redacted]	M. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name M. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

- TCP Session Timeout
  Normally, TCP sessions have a proper disconnect. However, in the event a server fails or reboots or the network breaks, the TCP session is going to timeout in the host. In this case, normal disconnect will not occur. Other means must be used to update the ECSC to the inactive state for this session. In the example shown in Figure A.11, the route to the TCP partner is disrupted by loss of a link or a node (1). The client TCP starts re-transmitting the same data. After reaching a threshold number of retransmissions (2,3,4), the client TCP timeouts and aborts the connection (5). Subsequently, the inactive timer in the PAD expires. The PAD updates the TCP session to an inactive state and reports the TCP session timeout error to the ECSC (7). The ECSC deletes the TCP session from its active session table and configures the PAD to stop marking the packets for the TCP session. The PAD deletes the state machine of the TCP session.



(Figure A.11 TCP Session Timeout Example)

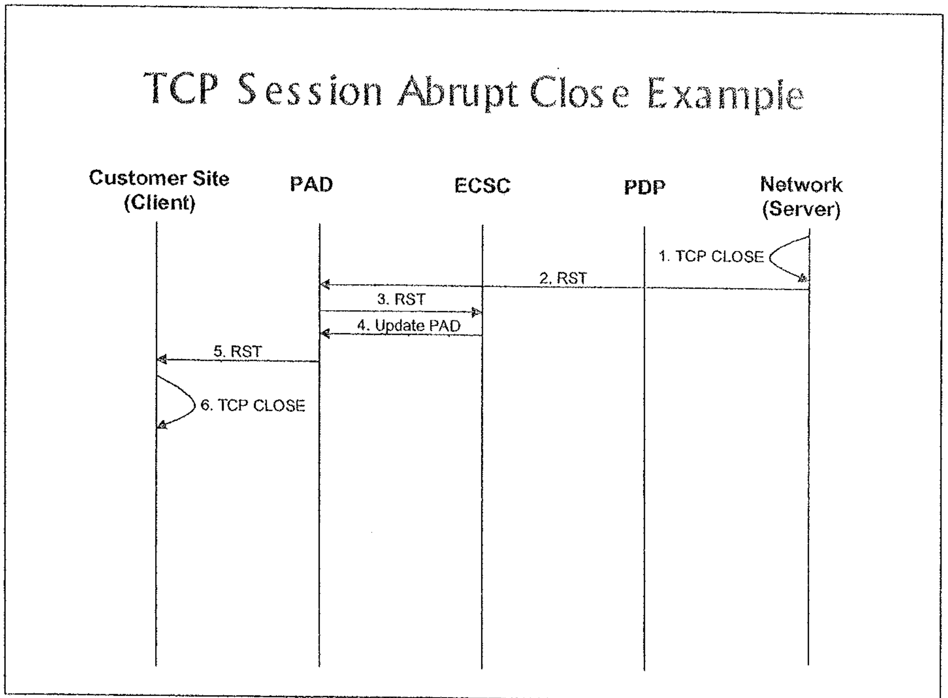
Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted] [redacted]

- TCP Session Abrupt Close

  Either side of a TCP connection can launch an abrupt close. This may be done because the application wishes to abort the connection, or because TCP has detected a serious communication problem that can not be resolved. An abrupt close is signaled by sending a RST segment to the partner. The server initiates the abrupt close in the example shown in Figure A.12 (1,2). The PAD resets the state machine for the TCP session to be idle and passes the RST segment to the ECSC (3). The ECSC deletes the TCP session from its active session table and configures the PAD to stop marking packets for this TCP session (4). The PAD deletes the state machine of the TCP session and forwards the RST segment to the client (5). The client closes the TCP session upon receiving the RST segment (6).



(Figure A.12 TCP Session Abrupt Close Example)

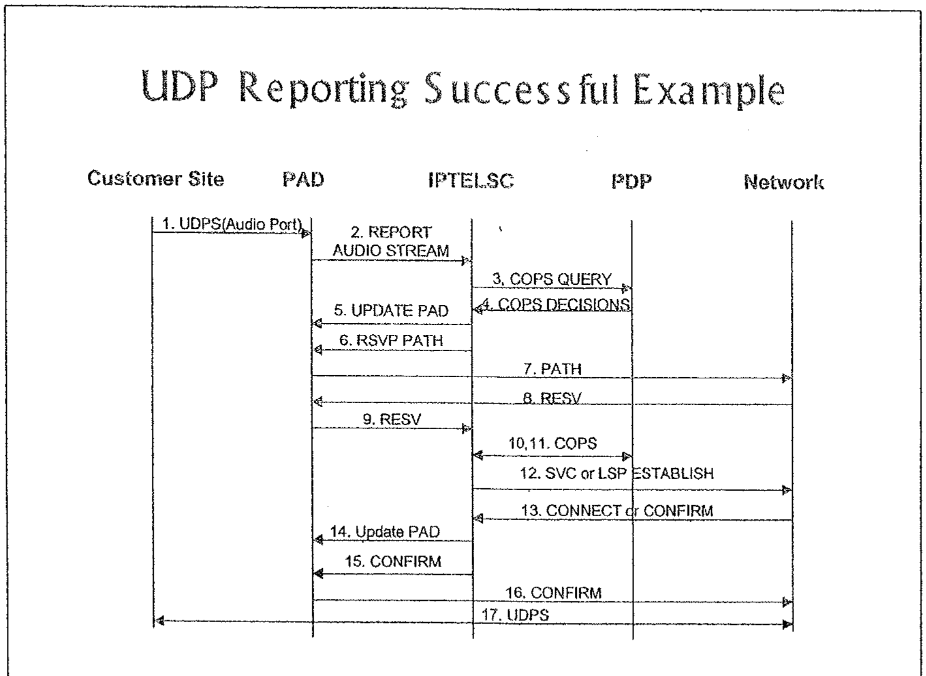
Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[redacted]	[redacted]	[redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted] [redacted]

A.5.3 Connection-less transport examples using UDP reporting function with specific port number ranges

- UDP Reporting Successful
  Section A.5.1 gives an example of RSVP signaling where the customer initiates the RSVP messaging. In the example shown below in Figure A.13, the client computer in the customer site does not support RSVP. A user on the customer site invokes a client program to make an IP telephone call. The client process gets an unused UDP port from the pool of available ports assigned for voice data transmission. The client application starts sending voice data encapsulated by UDP packets over the network as best-effort traffic (1). The PAD detects the constant flow of UDP packets (PT=17) within the voice port range and reports the occurrence of voice data flow to the IP Telephony Service Controller (IPTELSC) (2). The IPTELSC queries the PDP for policy decision (3) using COPS or some other policy query protocol. The PDP finds that the customer ordered guaranteed service for his IPTEL calls and commands the IPTELSC to provide guaranteed service for this IPTEL session (4). The IPTELSC configures the PAD with an inactive timer for this IPTEL call and instructs the PAD to stop reporting the occurrence of this IPTEL session. The IPTELSC initiates a reserved bandwidth route setup process (6-16). For an ATM core, a bi-directional SVC is set up. For an MPLS core, two uni-directional LSPs are set up. After the QoS path is established, all the voice UDP packets belonging to the IPTEL session are transmitted through the same QoS path (17). The PAD will periodically generate RSVP refresh messages on behalf of the user. If the IPTELSC caches enough policy information on making admission control decision in the first search (3,4), the IPTELSC does not need to query PDP for the second time and 10,11 are optional.

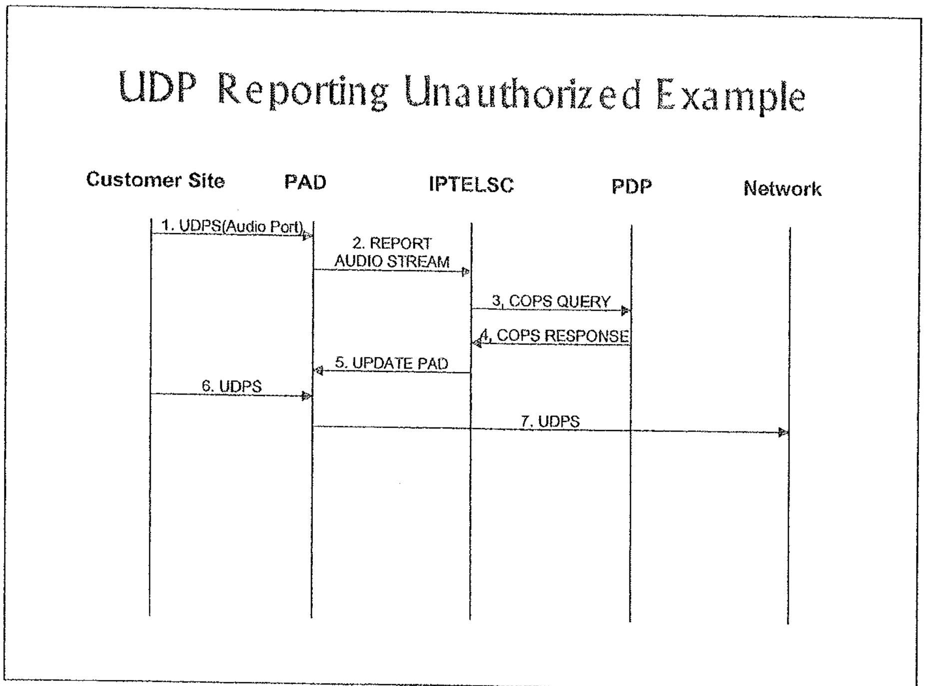


(Figure A.13 UDP Reporting Successful Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
	[redacted]		[redacted]		[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

- UDP Reporting Unauthorized

  In the example shown in Figure A.14, a user on a customer site invokes a client program to make an IP telephone call. The client process gets an unused UDP port from the pool of available ports assigned for voice data transmission. The client application starts sending voice data encapsulated by UDP packets over the network as best-effort traffic (1). The PAD detects the constant flow of UDP packets within the voice port range and reports the occurrence of voice data flow to the IP Telephony Service Controller (IPTELSC) (2). The IPTELSC queries PDP for policy decision (3) with COPS or some other policy query protocol. The PDP finds that there are no QoS requirements for this customer's IPTEL calls and sends only information response back to the IPTELSC (4). The IPTELSC configures the PAD to prevent the PAD from reporting the IPTEL call again and sets an inactive timer for this IPTEL call (When the inactive timer expires, the configuration the IPTELSC made on the PAD is cleaned.) The UPD packets are sent as best-effort traffic (6,7).



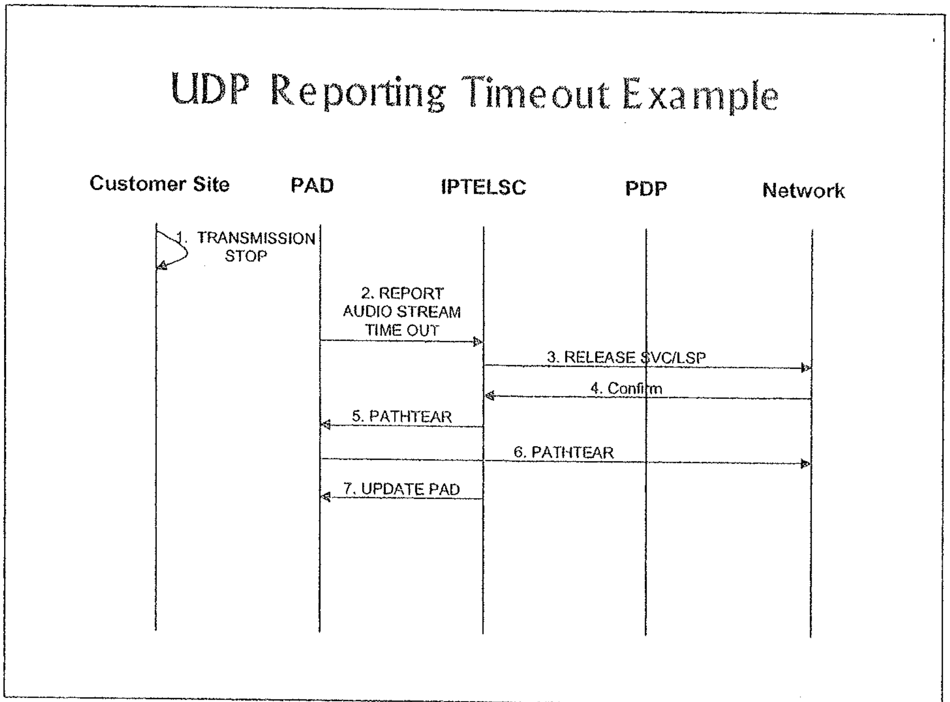
(Figure A.14 UDP Reporting Unauthorized Example)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted]

- UDP Reporting Timeout
  The UDP session inactive timer expiry can be caused either by normal completion of the UDP data flow, the break of the transmission links, or failure of the end computers. In the example shown in Figure A.15, the client application on the customer site has finished the call and stops sending voice traffic (1). The inactive timer for the IPTEL call expires after a while. The PAD detects the timeout event and reports it to the IPTELSC (2). The IPTELSC releases the SVC or LSPs for this call (3,4) and invokes the PATHTEAR to explicitly tear down the QoS path for the call (5,6). The IPTELSC then deletes this IPTEL call from its active session table. The IPTELSC configures the PAD to delete all the configured parameters for this call.



(Figure A.15 UDP Reporting Timeout Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

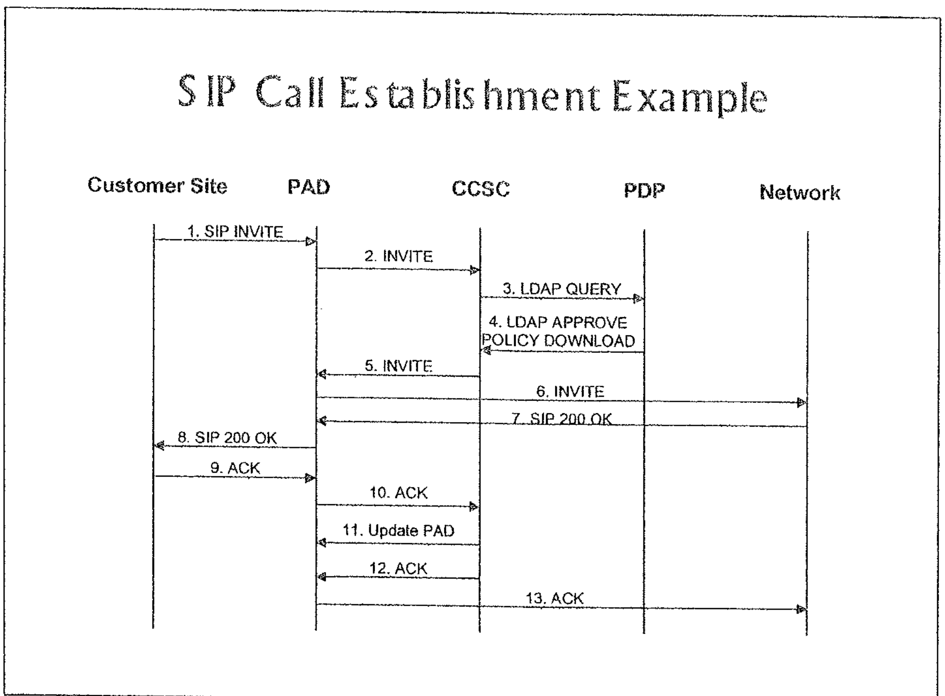
EXHIBIT A

[redacted]

A.5.4 Application-level examples using SIP signaling

[redacted], each SIP message invokes a policy query to approve a capability set. To reduce the number of messages exchanged between the SC and the PDP, the SC requests the PDP to dump the policy lookups for the SIP requester into its policy caches in its first policy query for a SIP call. The SC then uses the cached policies to make decisions for the SIP messages. The SIP state machine resides on the PAD. Thus the PAD is able to decide whether it needs to pass the received SIP message to the SC and should try to avoid forwarding SIP messages to the SC whenever possible.

- SIP Call Establishment
  In the example shown in Figure A.16, a caller on a customer site issues a SIP INVITE request to the callee (1). When the PAD detects the INVITE request (according to the UDP/TCP port range that is assigned to SIP), it passes the INVITE request to the Conference Call Service Controller (CCSC) (2). The CCSC sets the policy dump flag and queries the PDP for policy decisions using LDAP or some other policy query protocol (3). The PDP approves the SIP session (4) and dumps the policy lookups for the SIP caller into the policy caches of the CCSC. The CCSC returns the INVITE request to the PAD (5). The PAD forwards the INVITE request to the callee (6). The callee responds to the caller via 200 OK message (7). Since there is no change in the SIP capability set the PAD forwards the SIP 200 OK message directly to the caller (8) and does not pass it to the CCSC. The caller acknowledges the acceptance of the 200 OK message via an ACK request (9). The PAD passes the ACK request to the CCSC (10). The CCSC queries its policy caches and approves the final capability set of the SIP call. The CCSC adds the SIP session into its active session table and configures the PAD with an inactive timer and other parameters to facilitate the SIP call (11). The ACK is sent back to the PAD (12). The PAD in turn sends the ACK to the callee (13).



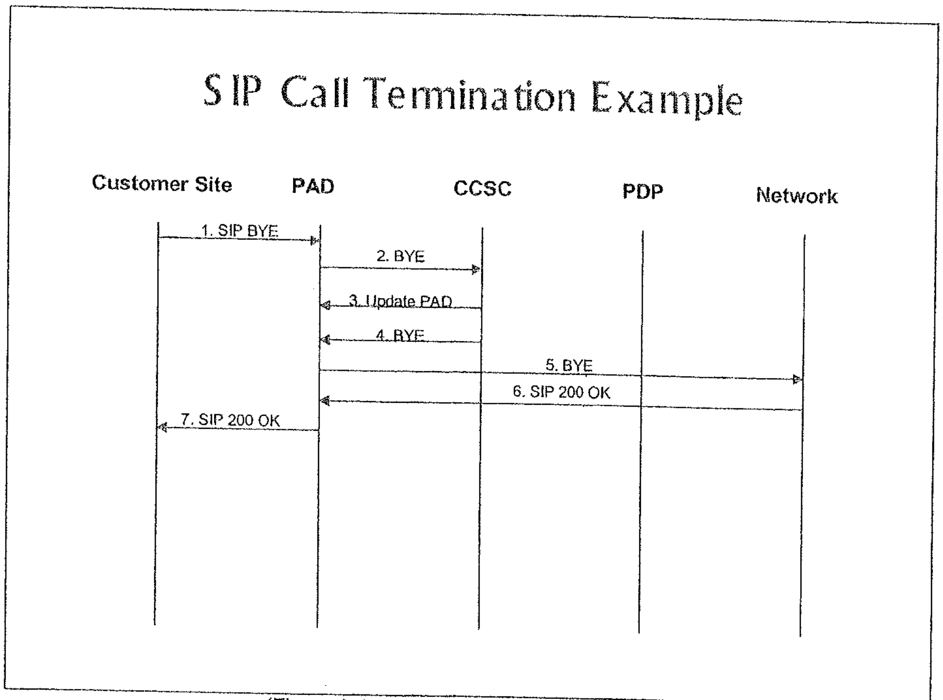
(Figure A.16 SIP Call Establishment Example)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[redacted]	[redacted]	[redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

- SIP Call Termination

  In a multi-party SIP conference call, each party can only drop himself from the call. After the last party leaves the call, the call is terminated. However, in a two-party SIP call, either the caller or the callee can terminate the call. Figure A.17 shows a two-party call termination example. The caller in the customer site signals the call termination by sending a BYE request (1). The PAD passes the BYE request to the CCSC (2). The CCSC deletes the SIP session from its active session table and cleans its policy caches. The CCSC then updates PAD to delete the entire configuration for the SIP call (3). The CCSC also prevents the PAD from passing subsequent SIP messages from the SIP call. The CCSC sends the BYE message back to the PAD (4). The PAD forwards the BYE message to the callee (5). The callee acknowledges the end of the SIP call via a SIP 200 OK message (6). The PAD forwards the 200 OK message to the caller without passing it to the CCSC (7).



(Figure A.17 SIP Call Termination Example)

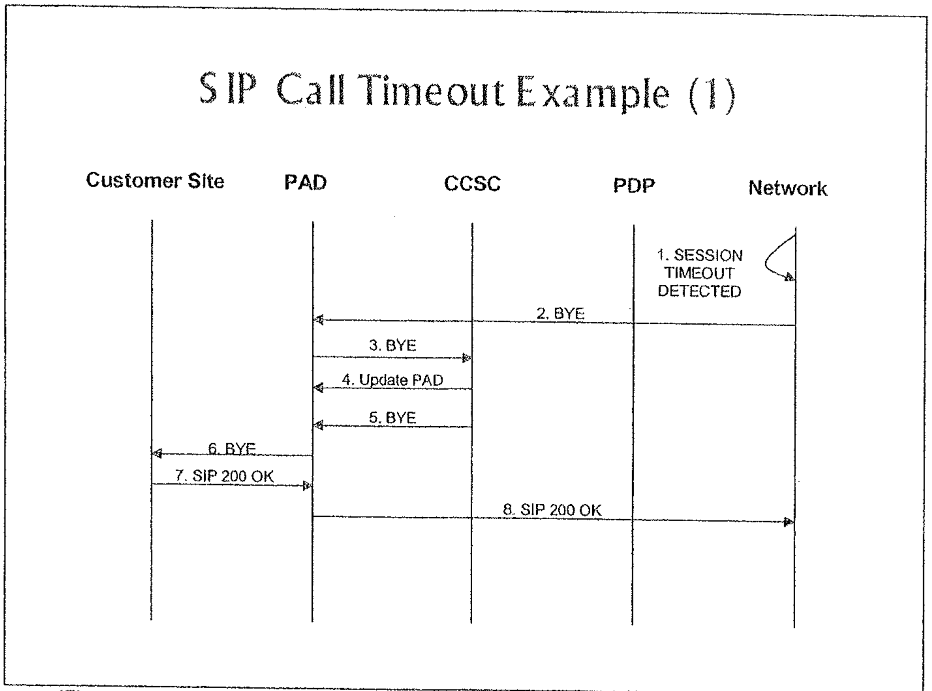
Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted]

- SIP Call Timeout

(1) In a SIP message, the ExpireTimer denotes the duration of the call before it expires. In the example shown in Figure A.18.1, the callee SIP application detects that the call has exceeded the allowed duration in ExpireTimer (1). The callee then issues a BYE request (2). The PAD passes the BYE request to the CCSC (3). The CCSC deletes the SIP session from its active session table and cleans its policy caches. The CCSC commands the PAD to delete the entire configuration for the SIP call (4). The CCSC also prevents the PAD from passing it subsequent SIP messages from the SIP call. The CCSC returns the BYE request to the PAD (5). The PAD forwards the BYE request to the caller (6). The caller acknowledges the end of the SIP session via a SIP 200 OK message (7). The PAD forwards the OK message to the callee (8).



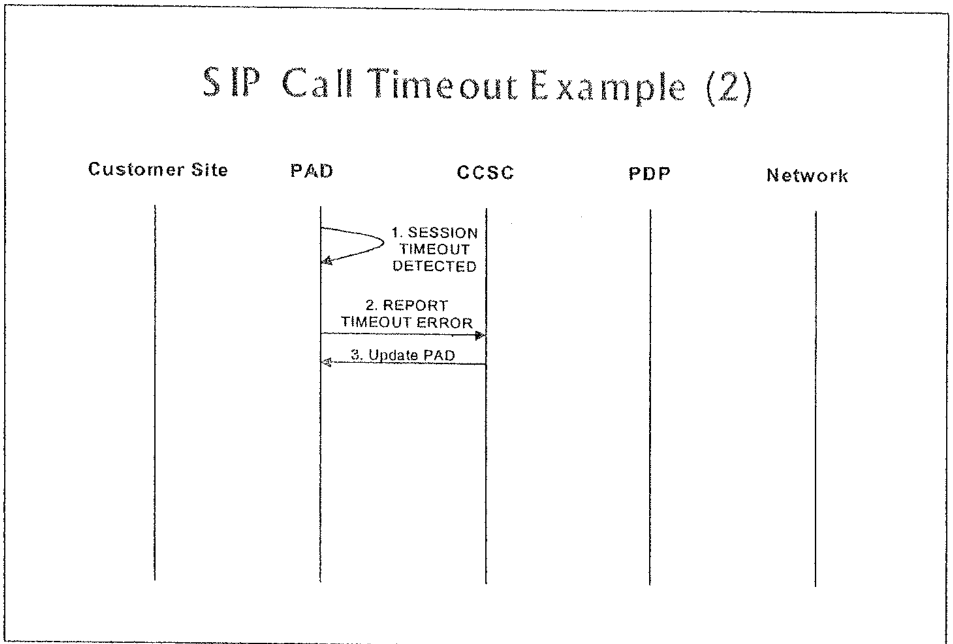
(Figure A.18.1 SIP Call Timeout Example (1)--- timeout detected by the SIP application)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted] [redacted]

(2) In the example shown in Figure A.18.2, all parties of the SIP call die. The inactive timer of the SIP call expires (1). The PAD reports the timeout error to the CCSC (2). The CCSC deletes the SIP session from its active session table and cleans its policy caches. The CCSC commands the PAD to delete the entire configuration for the SIP call (3).



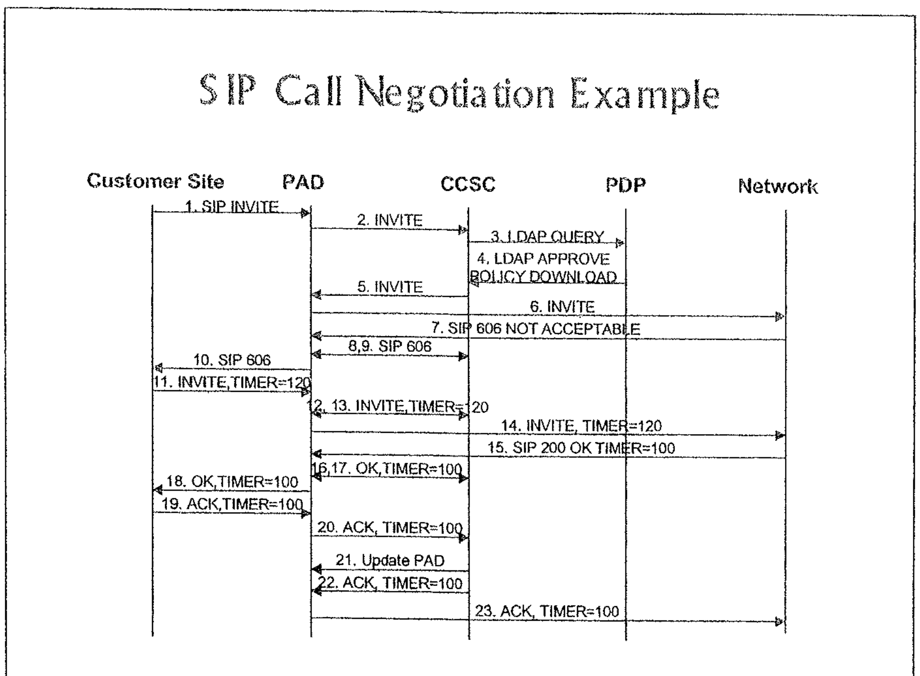
(Figure A.18.2 SIP Timeout Example (2)--- All parties in the SIP call die and timeout is detected by PAD)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDyson [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDyson	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

[redacted] [redacted]

- SIP call negotiation
  In the example shown in Figure A.19, a caller on a customer site issues a SIP INVITE request to the callee (1). The PAD passes the INVITE request to the CCSC (2). The CCSC sets the dump policy flag and queries the PDP (3) with LDAP or some other policy query protocol. The PDP approves the SIP session and dumps policy lookups for the SIP call into the policy caches of the CCSC (4). The CCSC returns the INVITE request to the PAD (5). The PAD sends the INVITE request to the callee (6). Since the INVITE request specifies a bandwidth that is higher than what can be supported by the access link of the callee and requests a set of media encodings, the callee responds with a 606 Not Acceptable message (7). The response states that only 56 Kbps is available and that only PCM or LPC audio could be supported in order of preference. When the 606 response is passed to the CCSC (8), the CCSC queries its local policy caches and approves the new capability set. The CCSC sends the 606 response back to the PAD (9). The PAD forwards the 606 response to the caller (10). When the caller receives the 606 response, it adjusts the call capability requirements and issues another INVITE request (11), which specifies 56 Kbps bandwidth, LPC audio encoding and the ExpireTimer 120 minutes. The PAD passes the new INVITE request to the CCSC (12). The CCSC queries its local policy caches and approves the new SIP capability set again. The CCSC returns the INVITE request to the PAD (13). The PAD sends the INVITE request to the callee (14). The callee is able to support all the call requirements except that it requires the call duration to be 100 minutes. The callee responds a 200 OK response with the ExpireTimer 100 minutes (15). The PAD passes the OK response to the CCSC (16). The CCSC checks the SIP capability set carried in the OK response and approves it. The CCSC then sends back the OK response to the PAD (17). The PAD forwards the OK response to the caller (18). When the caller receives the OK response it modifies its ExpireTimer requirement to be 100 minutes and acknowledges via an ACK request (19). The PAD passes the ACK response to the CCSC (20). The CCSC approves the final SIP capability set carried in the ACK response. The CCSC configures the PAD with an inactive timer and other parameters to facilitate the SIP call (21). The CCSC then returns the ACK to the PAD. The PAD forwards the ACK to the callee. After the callee receives the ACK response, the SIP call is successfully established.



(Figure A.19 SIP Call Negotiation Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted]

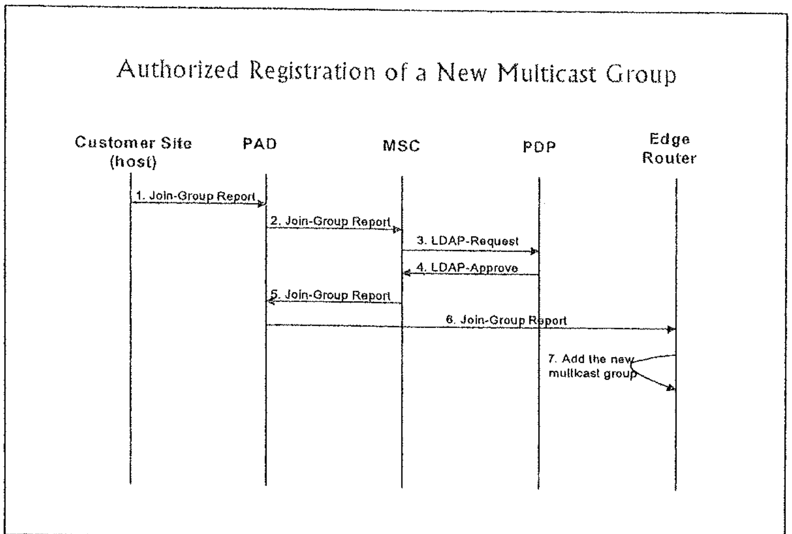
A.5.5 IP Multicast Examples

The current IP multicast uses an open group model.[redacted] Multicast group members can join or leave a multicast group at will. There is no need to register, synchronize, or negotiate with a centralized group management entity. However for a multicast service, the customers expect control and management of group membership for both the sender and receiver.[redacted]

The proposed access system architecture in this petition enables policy-based multicast service management by monitoring the IGMP messages.

- Manage the registration of the new multicast groups

(1) Authorized Registration of a new multicast group
In the examples shown in figure A.20.1, a host on the customer site signals an IGMP join-group Report message to the edge router (1) (on the right hand side of figure A.20.1). IP filter in the PAD captures the IGMP messages based on PT=2. The PAD forwards the join-group Report message to the Multicast Service Controller (2) (MSC). The MSC queries the PDP within the policy database with LDAP or some other policy query protocol (3). The PDP finds the sender's IP address in the eligible membership list and approves that the sender join the group (4). The Membership Report message is forwarded to the edge router (5,6). In case the sender is the first member of that group on the network, the router adds the group being reported to the list of multicast group memberships on the network on which the sender is attached (7).



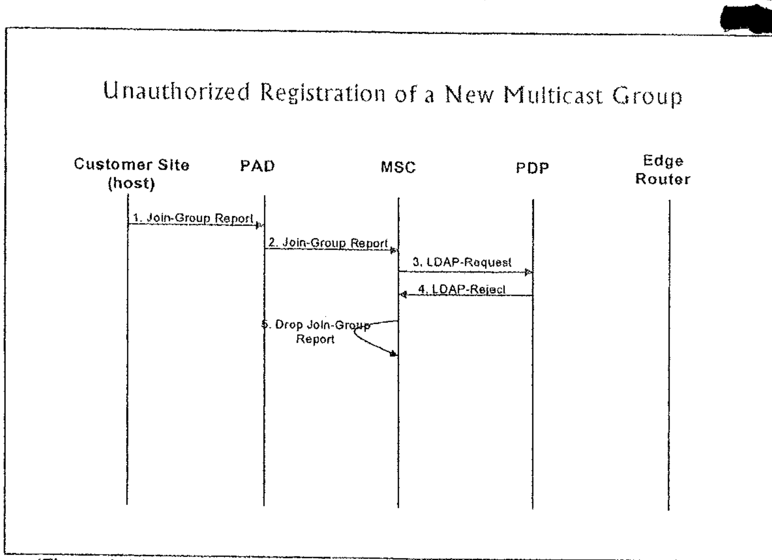
(Figure A.20.1 Authorized Registration of a new multicast group Example)

(2) Unauthorized Registration of a new multicast group
In the examples shown in figure A.20.2, a host on the customer site signals an IGMP join-group Report message to the edge router (1) (on the right hand side of figure A.20.2). The IP filter in the PAD captures the IGMP messages based on PT=2. The PAD forwards the join-group Report message to the Multicast Service Controller (2) (MSC). The MSC queries the PDP within the policy database with LDAP or some other policy query protocol (3). The PDP finds that the sender is not eligible to join the multicast group and rejects the join-group request (4). The MSC drops the join-group Report message and write into its event log a warning message (5). This prevents the unauthorized host from registering a new group in the edge router.

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

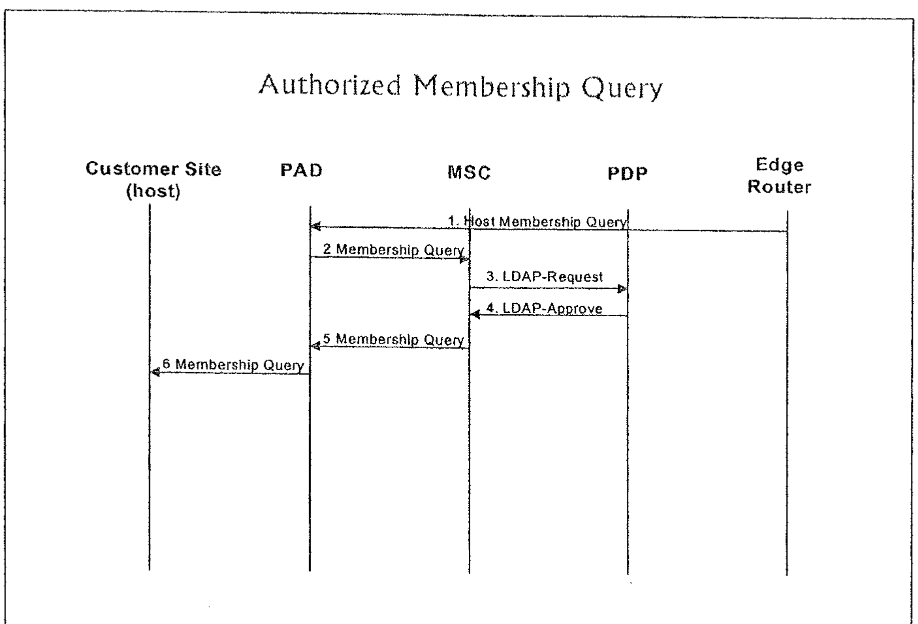
[redacted]



(Figure A.20.2 Unauthorized Registration of a new multicast group Example)

- Manage the host membership queries

(1) Authorized Membership Query
In the example shown in figure A.21.1, the PAD receives an IGMP host membership Query message from the edge router (1). It passes the host membership Query message to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds the source address for this query is the authorized edge router and PDP approves the Query (4). The host membership Query message is forwarded to the hosts in the customer site/sub-network (5,6).



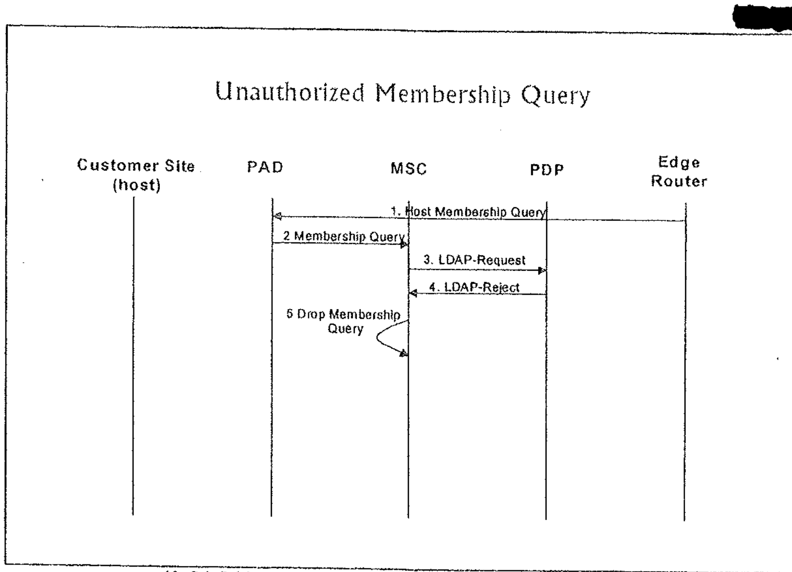
(A.21.1 Authorized Membership Query Example)

(2) Unauthorized Membership Query
In the example shown in figure A.21.2, the PAD receives an IGMP host membership Query message (1). It passes the host membership Query message to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the Query is from an unidentified or unauthorized source and rejects the Query (4). The MSC drops the Query message and writes a warning message into its event log (5). This prevents the denial of service attack by fake host membership Query messages.

Inventor Signature / Date	Inventor Signature / Date	Inventor Signature / Date
David E. McDysan [redacted]	H. Lee Thomas [redacted]	Lei Yao [redacted]
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

EXHIBIT A

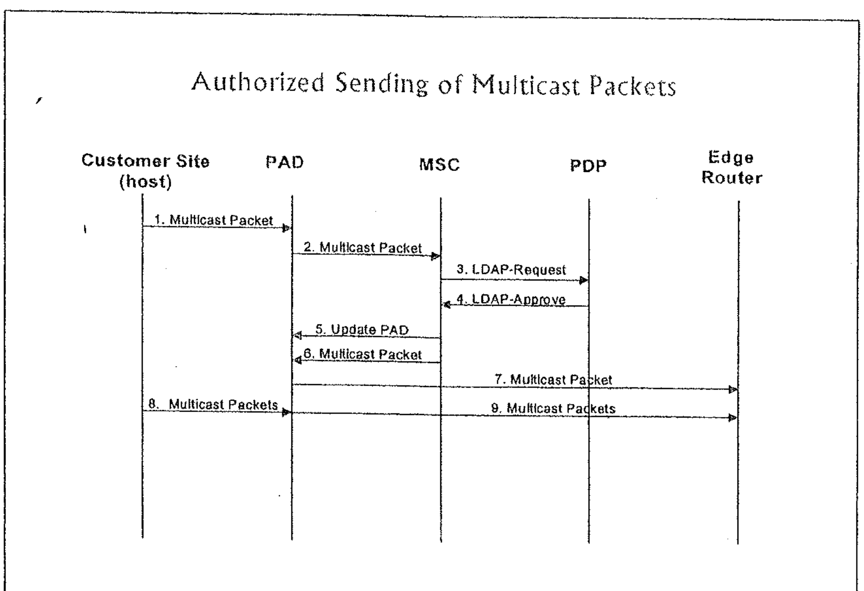
[redacted]



(A.21.2 Unauthorized Membership Query Example)

- Manage the sending of multicast packets to the network

(1) Authorized sending of multicast packets to the network
In the example shown in figure A.22.1, a host on a customer site sends IP multicast packets to the multicast groups. When the PAD receives the first multicast packet (1), the IP filter captures the packet by checking its multicast address. The PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the source address of the IP multicast packet is authorized for sending multicast packets to the multicast group and approves the sending of the multicast packet (4). The MSC configures the PAD to directly forward multicast packets to the edge router for the (source, multicast address) pair (5) and returns the first multicast packet to the PAD (6). The PAD forwards the multicast packet to the edge router (7). The PDP forwards all the following multicast packets for the flow directly to the edge router without passing to the MSC (8,9).



(Figure A.22.1 Authorized sending of multicast packets Example)

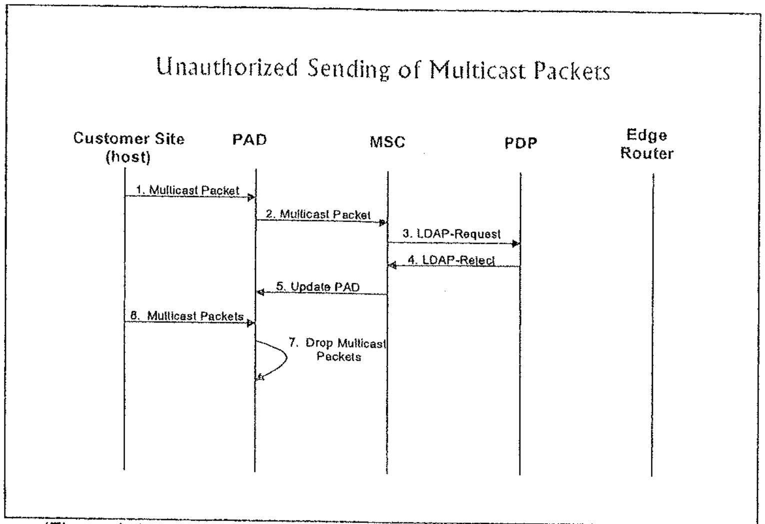
(2) Unauthorized sending of multicast packets to the network
In the example shown in figure A.22.2, a host sends IP multicast packets to the multicast groups. When the PAD receives the first multicast packet (1), the IP filter captures the packet by checking its multicast address. The PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the source sending the multicast

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

[redacted]

packets is unidentified or unauthorized and rejects the sending of multicast packets to the network (4). The MSC configures the PAD to drop multicast packets for the (source, multicast address) pair and writes a warning message into the event log (5,6,7). This prevents the denial of service attack by flooding multicast packets onto the network.



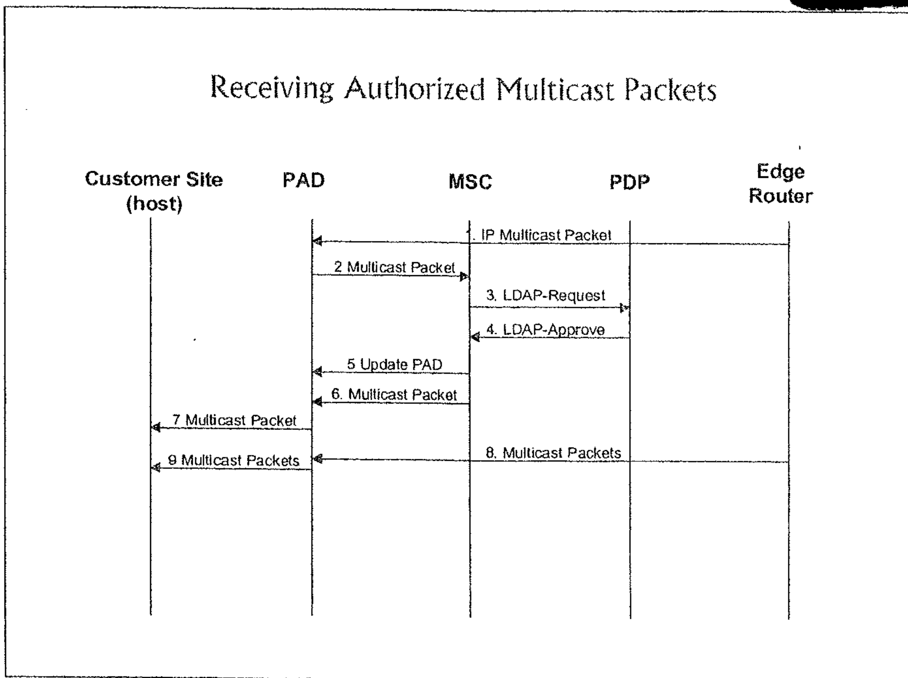
(Figure A.22.2 Unauthorized sending of multicast packets Example)

- Manage the receiving of multicast packets from the network

(1) Receiving authorized multicast packets
In the example shown in figure A.23.1, the edge router receives IP multicast packets from the network and forwards them to the PAD. When the PAD receives the first multicast packet from the edge router (1), the PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the source address of the IP multicast packet was authorized for sending multicast packets to the multicast group and approves forwarding the multicast packet to multicast hosts in the customer site (4). The MSC configures the PAD to directly forward to the edge router multicast packets for the (source, multicast address) pair (5), and returns the first multicast packet to the PAD (6). The PAD forwards the multicast packet to the multicast hosts in the customer site (7). The PAD forwards all the following multicast packets for the flow directly to the multicast hosts in the customer site without passing to the MSC (8,9).

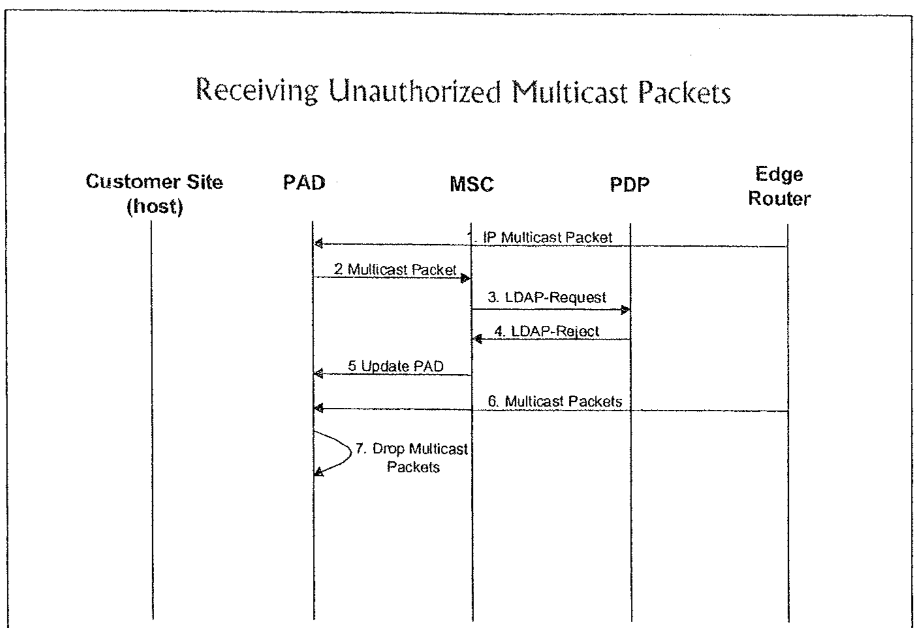
Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	[redacted]	H. Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A



(A.23.1 Receiving Authorized Multicast Packets Example)

(2) Receiving unauthorized multicast packets
In the example shown in figure A.23.2, the edge router receives IP multicast packets from the network and forwards them to the PAD. When the PAD receives the first multicast packet from the edge router (1), the PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PAP finds that the source sending the multicast packets is unidentified or not authorized and rejects forwarding the multicast packet to the multicast hosts in the customer site (4). The MSC configures the PAD to drop multicast packets for the (source, multicast address) pair and write a warning message into the event log (5,6,7). This prevents the unauthorized multicast packets from flooding the sub-network in the customer site.



(A 23.2 Receiving Unauthorized Multicast Packets Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	[redacted]	H Lee Thomas	[redacted]	Lei Yao	[redacted]
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

EXHIBIT A

ACRONYMS

ACK	Acknowledgement
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CCSC	Conference Call Service Controller
COPS	Common Open Policy Service
CPE	Customer Premise Equipment
CPU	Central Processor Unit
DA	Destination Address
Diffserv	Differentiated Services
DP	Destination Port Number
DSCP	Diffserv Codepoint
ECSC	E-Commerce Service Controller
FAST	First ATM SVC Trial
FIN	Finished
FR	Frame Relay
IGMP	Internet Group Multicast Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPTEL	IP Telephony
IPTELSC	IP Telephony Service Controller
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LPC	Linear Predictive Coding
LSP	Label Switched Path
MCIW	MCI WorldCom
MCRI	Message, Control, and Reporting Interface
MPLS	Multiprotocol Label Switching
MSC	Multicast Service Controller
PAD	Programmable Access Device
PADC	Programmable Access Device Controller
PANDSC	Programmable Access Device with Distributed Service Control
PDP	Policy Decision Point
PNNI	Private Network-Network Interface
POP	Point of Presence
PT	Protocol Type
PVC	Permanent Virtual Connection
QoS	Quality of Service
RBS	Reserved Bandwidth Service
RBSC	Reserved Bandwidth Service Controller
RST	Reset
RSVP	Resource Reservation Protocol
RTP	Real-time Transport Protocol
SA	Source Address
SBM	Subnet Bandwidth Manager
SC	Service Controller
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SP	Source Port Number
SPI	Service Policy Interface
SVC	Switched Virtual Connection
SYN	Synchronizing segment
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TOS	Type of Service
UDP	User Datagram Protocol
UNI	User Network Interface
WAP	Wireless Application Protocol

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
		Lei yao [redacted]
Print Name	Print Name	Print Name LEI YAO

EXHIBIT A

[redacted]

From: Lei Yao[redacted]]
Sent: [redacted]
To: 'Brian F. Russell'
Cc: 'Dave.mcdysan'; 'steven.mccann'; lee.thomas[redacted]; jim.dalton[redacted]
Subject: RE: patent application

ric.zip

Brian,

Attached please find our consolidated comments. We divided the comments into general comments and detailed comments. The general comments are put into a separate document. Detailed comments are made in the draft document with our initials. We also made some changes in the drawings.

Below is the conference bridge info.:
Date: [redacted]
Time: [redacted] (EDT)
Toll Free - [redacted]
Pass Code [redacted]

EXHIBIT B

Thanks again for your excellent work.

Lei

-----Original Message-----
From: Brian F. Russell [redacted]
Sent: [redacted]
To: lei.yao
Cc: Dave.mcdysan; steven.mccann
Subject: RE: patent application

<< File: RIC00033 (44796).doc >> << File: landscapedrawings.doc >> << File: portraitdrawings.doc >> Gentlemen,

Please find attached an initial draft of the first patent application. I would appreciate it if you could forward a copy to Lee for his review, as I don't have his email address.

I will continue working on the claims for the 3 additional applications while I await your comments. As you work through the document, please address the highlighted comments embedded in the text. Also, please consider whether the description is technically accurate and complete (whether it discloses to a person "skilled in the art" how to make and use the invention) and discloses the "best mode", if any, in which the invention may be used.

It would be helpful to me if comments for all the inventors can be compiled into either a single marked up version of the application or a single set of separate comments. Thank you for your assistance in the preparation of this application, and please contact me if I can resolve any issues that arise during the review process.

Best regards,

EXHIBIT C

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731

[redacted]

[redacted] (voice)
[redacted] (fax)
[redacted]
www.patentlawyers.com

>>> Lei Yao <[redacted]> [redacted]

EXHIBIT D

Brian,

Thanks for the update. We are looking forward to read the application.

Lei

-----Original Message-----
From: Brian F. Russell [[redacted]]
Sent: [redacted]
To: lei.yao
Cc: Dave.mcdysan; steven.mccann
Subject: RE: patent application

Lei,
Just to update you on my progress on the applications, I have nearly completed a draft of the first application and expect to send you the draft for review next week. As we discussed, the all of the applications will contain the same basic description, but will differ in focus in the claims, summary and abstract. Hopefully, the commonality in the applications will facilitate your review.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
[redacted] (voice)
[redacted] (fax)
[redacted]
www.patentlawyers.com

EXHIBIT E

[redacted]

From: Brian F. Russell [redacted]
Sent: [redacted]
To: dave.mcdysan; lei.yao
Cc: lee.thomas; steven.mccann
Subject: RE: patent application

Gentlemen,

Just to update you on the status of the patent applications, I have unfortunately been unable to work on the patent applications since I received the information Dave McDysan provided because of additional duties I have had to assume since Andrew, the firm's managing partner, broke his back last weekend.

Originally, I had anticipated completing all of the applications by [redacted]. I now believe that I can have revised drafts of the applications to you for review by [redacted].

I apologize for the delay.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
[redacted] (voice)
[redacted] (fax)
[redacted]
www.patentlawyers.com

EXHIBIT F

[redacted]

[redacted]

From: Brian F. Russell [[redacted]]
Sent: [redacted]
To: dave.mcdysan; lei.yao
Cc: lee.thomas; steven.mccann
Subject: RE: patent application RIC00043

Follow Up Flag: Follow up
Flag Status: Completed

RIC00043.cla.doc

Gentlemen,
Attached please find the claims, abstract and summary for the external processor application.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
[redacted] (voice)
[redacted] (fax)
[redacted]
www.patentlawyers.com

EXHIBIT G

[redacted]

From:	Brian F. Russell [[redacted]]
Sent:	[redacted]
To:	dave.mcdysan; lei.yao
Cc:	lee.thomas; steven.mccann
Subject:	RE: patent application RIC00033
Follow Up Flag:	Follow up
Flag Status:	Completed

landscapedrawings.doc | Overview.ppt | portraitdrawings.doc | RIC00033 (44796).doc | RIC00042.cla.doc

Gentlemen,

Attached, please find attached the following:

(1) the second draft of the patent application, which includes your most recent comments [Please see my imbedded notes and questions pertaining to the "Overview" description that was added] and a full claim set;
(2) figures for the application (which are unchanged except for the insertion of reference numerals in the "Overview" drawings provided by Dave);
(3) claims, abstract and summary for the second application covering the PAD (Docket No. RIC00042).

I will send the claims, abstract and summary for the other two applications either later today or tomorrow.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
[redacted] (voice)
[redacted] (fax)
[redacted]
www.patentlawyers.com

EXHIBIT H

[redacted]

[redacted]

From: LEI YAO [[redacted]]
Sent: [redacted]
To: 'Brian F. Russell'; dave.mcdysan
Cc: lee.thomas; steven.mccann
Subject: RE: patent application RIC00044

EXHIBIT I

Brian,

Thanks for putting together all four applications during the short period.

Steven,

I will coordinate with Dave and Lee to review these applications. After the applications have been agreed on by us, do we need approval from you before we really submit these applications? What is the next step from the legal department?

Thanks.
Lei

-----Original Message-----
From: Brian F. Russell [redacted]
Sent: [redacted]
To: dave.mcdysan; lei.yao
Cc: lee.thomas; steven.mccann
Subject: RE: patent application RIC00044

<< File: RIC00044.cla.doc >> Gentlemen,

Please find attached the claims for the final patent appliication covering the MCRI.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
[redacted] (voice)
[redacted] (fax)
[redacted]
www.patentlawyers.com

EXHIBIT J

[redacted]

From: LEI YAO [redacted]
Sent: [redacted]
To: 'paul.roberts[redacted]'; 'Steven.McCann[redacted]
Cc: 'dave.mcdysan[redacted]'; 'brussell[redacted]'; 'lee.thomas[redacted]
Subject: patent applications

patentcmts.zip

Paul,

Attached please find the final comments we made for the patent applications prepared by Brian Russell. We understand that you will work on this case representing Steven. The applications were well written. We only made several minor changes. If you turn on "track change" options of MS Words, you should be able to see those changes. We believe that the applications are ready to be submitted. [redacted]

Please let us know your thoughts.

Thank you very much.
Lei

EXHIBIT K

[redacted]

[redacted]

From:	Brian F. Russell [redacted]
Sent:	[redacted]
To:	lei.yao
Cc:	dave.mcdysan; lee.thomas; Paul.roberts
Subject:	Re: Patent applications

Gentlemen,

Thank you for your assistance in preparing the patent applications. I have reviewed the comments you had and have finished incorporating them into the applications.

To speed up preparation of the legal documents that will accompany the applications, I need updated addresses for each of you (the ones listed in the disclosure seem to be out of date).

Thank you for your help.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
[redacted] (voice)
[redacted] (fax)
[redacted]
www.patentlawyers.com

EXHIBIT L

[redacted]

MAY 1 2001

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/723,501	11/28/2000	2661	1128	RIC00043	21	36	2

CONFIRMATION NO. 7593

UPDATED FILING RECEIPT

OC000000006005761

25537
MR. PAUL ROBERTS
MCI WORLDCOM
1133 19TH STREET NW (9854/003)
WASHINGTON, DC 20036

Date Mailed: 04/25/2001

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Dave McDysan, Herndon, VA;
Howard Lee Thomas, Ballwin, MO;
Lei Yao, Arlington, VA;

Domestic Priority data as claimed by applicant

Foreign Applications

If Required, Foreign Filing License Granted 03/29/2001

EXHIBIT M

Projected Publication Date: N/A

Non-Publication Request: No

Early Publication Request: No

Title

External processor for a distributed network access system

Preliminary Class

370

MCI WORLDCOM. Invention Disclosure Form

Item 1. Provide a short, descriptive title of the invention:
Distributed Programmable Access Device Network Supported by Separate Service Controllers

Item 2a. When and under what circumstances was the invention first conceived (if you have any written evidence of this date, include copies):
The invention was born out of initiatives within the Company to provide customers with integrated access to all Company services and to provide customers with dynamic capabilities to adjust their services, either in type or quantity. The inventors work in the Next Generation Switching and Control group and developed this invention while working on various projects directed toward pushing network intelligence and integrated access to the edge of the network and separating switching and routing from control functions throughout the network.

Item 2b. What is the date of the first sketch or drawing of the invention:
January 4, 2000

Item 2c. What is the date of the first written description of the invention:
January 4, 2000

Item 2d. What is the date of the first test of or operation of the invention:
Not Applicable.

Item 3a. List all contributors (use other pages if necessary) to this conception of the invention and indicate the contributor's company if not an MCI WorldCom employee (also identify one person as a primary contact with an "X" next to the name):

X Printed Name: ___McDysan__________ David__________ E.________
Last name / First / Middle initial

***Please record your name correctly: Last Name, First Name, Middle Initial; DO NOT USE NICKNAMES, etc.**

Phone#: (w) _972.729.1288 (h) ______ Dept/Loc: _2042/____ E-MailID: __dave.mcdysan@wcom.com___

Current Address: __901 International Place___Richardson_____Texas______75081____
Street / City / State / Zip code

Country: __USA____ Citizenship: ____USA____ Job Title: _____Fellow________

Job assignment at invention conception: ________Next Generation Switching________

Printed Name: ___Thomas__________ H.__________ Lee________
Last name / First / Middle initial

Phone#: (w) _314.216.1308 (h) _314.256.7112 Dept/Loc: _2042/XA5___ E-MailID: _lee.thomas@wcom.com____

Current Address: _One Brooks Center Parkway, Town&Country_____MO______63017____
Street / City / State / Zip code

Country: ___USA____ Citizenship: ___USA____ Job Title: _____Senior Engineer________

Job assignment at invention conception: __________Next Generation Switching________

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E McDysan		Print Name H Lee Thomas		Print Name LEI YAO	

MCI WORLDCOM Invention Disclosure Form

Printed Name: ___Yao________________________Lei________________________________
Last name First Middle initial

Phone#: (w) _703.886.1830_ (h) _____________ Dept/Loc: _2042/ ___ E-MailID: _lei.yao@wcom.com_______

Current Address: _22001 Loudoun County Parkway, Ashburn_________VA__________________20147___________
Street City State Zip code

Country: ___USA_________ Citizenship: ___China______ Job Title: _____ Engineer__________________

Job assignment at invention conception: __________Next Generation Switching_______________________________

Item 3b. Provide the management chain (through VP) of the originating organization for the invention:
Dave Mcdysan
Vint Cerf, Sr. VP

Thomas Lee, Lei Yao
Jim Dalton, Sr. Manager
Chris Daniel, Director
Hack Kim, Sr. VP

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E McDysan 4/27/00	H Lee Thomas 5/01/00	Lei Yao 5/02/00
Print Name David E. McDysan	Print Name H Lee Thomas	Print Name LEI YAO

Item 8. Describe the invention using the following format. Use as many pages as necessary. **Mark each additional page "MCI WorldCom Confidential."**

1. Discuss the problems which the item is designed to solve. Refer to any prior devices of a similar nature with which you may be familiar.

   A. Today's routers implement the routing, forwarding, policy, policing, marking, and admission control functions in a monolithic, proprietary manner. A few routers have limited implementation of external policy control. The services that a provider can offer are limited by the control software implemented by a particular router/switch vendor. If a service provider has routers from multiple vendors in a network, the proprietary services will not inter-operate. Consequently, the service provider is not able to purchase router/switches from one vendor and purchase policy-based service control from another vendor. Furthermore, a service provider cannot offer its network as a platform for a wholesale provider to offer value-added services utilizing the existing base network capabilities.

   B. The implementation of the multiple functions listed above in a monolithic router presents a significant scalability challenge for vendors in response to the phenomenal growth of Internet traffic. The current design approach by the industry separates the problem into core and access routers. Access routers perform the most complex functions and perform operations that simplify the tasks required of core routers. However, the monolithic design of access routers presents a limit for scalability of the Internet. Evidence of this fact is that the access router software image size is increasing.

   C. Another problem brought on by the rapid growth of Internet traffic is the need to dynamically provision, configure, and/or reallocate access capacity to IP-based services. Access capacity is often limited and a major cost component of modern networks. Therefore, it is subject to congestion and has a strong need for admission control and different levels of quality. Also, access products are not capable of handling a wide variety of traffic types while being able to enforce policy controls (provider-initiated or customer-initiated) or dynamic requests for capacity.

   D. Today's routers cannot distinguish between higher layer message types and forward the higher layer messages according to service/policy parameters. Today's routers do not use a combination of protocol type, source IP address (SA), destination IP address (DA), type of service (TOS) or differentiated service code-point (DSCP), source port number (SP) and destination port number (DP) to distinguish different message types. In fact, most routers use only the DA to make the forwarding decision. Some newer routers use only DA plus TOS/DSCP.

   E. Today's access routers have a concept of one controller providing all services for all message types. This results in a single complex router, which is difficult to add new services or modify existing services. This monolithic design limits flexibility and extensibility and increases cost. Evidence of this fact is that the time to market for new features and functions are delayed. For example, in today's network, if a service provider's external policy server sends COPS messages to an access router, the service provider must ask the vendor to develop a COPS interface on the router.

   F. Today's routers have relatively weak security control of their configuration information. For example, a command line interface is invoked by a simple userid password exchange in the clear when initiating over a telnet session.

   G. Desktop computing applications provide customers with the means to utilize many different services while each service requires different (quality of) service requirements. Today's networks do a poor job of identifying which traffic is associated with which service. Therefore, applications vie for whatever network resources can be obtained in a first-come, first-served fashion.

   H. Traffic patterns are shifting from the traditional telecommunications model where the community of interest was primarily local to one where the community of interest is distance independent.

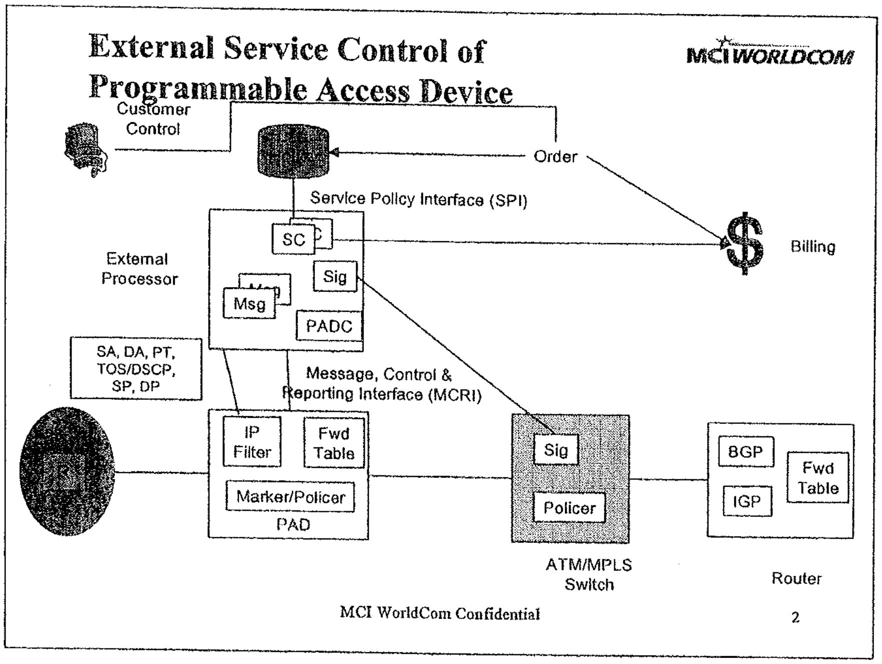
   I. Today's network is not able to measure or monitor the statistics of layer-2 and layer-3 traffic types and take advantage of dynamic network capabilities to add network resources to support customer Service Level Agreements (SLAs).

   The invention is similar to FAST with respect to the separation of signaling and switching and interaction with policy servers. This disclosure extends these concepts to IP connectionless protocols as well as higher layer session and application layer protocols.

2. Describe how the invention qualifies as a solution to the problem, and state the advantage of the item over presently known devices, systems or processes.

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan 4/27/00	H. Lee Thomas 5/01/00	Lei Yao 5/02/00
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

A. The invention decomposes the traditional router into a Programmable Access Network with distributed service control (PANDSC) and hardware/software Service Controllers (SC) executing on external processors as shown in Figure 1. The SCs interface to the PAD using a Message Control and Reporting Interface (MCRI). The PAD uses the MCRI to pass service-specific messages to/from the corresponding service controller software/hardware executing on an external processor. The PAD uses fields in the network, transport and application layer headers to identify a particular traffic flow and determine which messages are passed to a specific service controller. One or more service controllers may remotely control a single PAD; however, only one SC would control a particular traffic flow. Additionally, the PAD can report on events of statistics of received traffic according to parameter ranges and intervals defined by the SC. The combination of the PAD functions of service-specific message forwarding, remote control, and reporting enables the implementation of the service controllers by different vendors than those implementing the PAD.



B. The invention achieves superior scalability when compared with traditional routers since it separates out the functions performed by a router into three platforms. Routing is still done in the router as shown on the right-hand side of Figure 1. However, the functions of filtering, message forwarding, policing, and marking are placed in the PAD. Finally, the message interpretation, signaling, admission control, and policy invocation is implemented in SCs on external processors.

C. The Programmable Access Device and SC enable customer applications to reserve bandwidth, perform admission control, and prioritize traffic streams based upon available capacity and policy controls. These policy controls may be initiated by the provider or the customer organization. The capability for customer applications to interact with service provider network resources provides the customer the ability to dynamically provision services as well as provide applications the required quality of service guarantees. If the PAD is located at the extreme edge of the network, then the external processor can signal for access capacity. This network-based provisioning invoked by policy control replaces time-consuming and error-prone OSS provisioning.

D. The IP filter in the PAD provides the ability to identify higher layer message types (network, transport and application layers) and forward those messages from/to the external processor based on the parameters configured by message processor. The IP filter will have the ability to use a combination of protocol type, SA, DA, TOS or DSCP, SP, DP and other fields to distinguish different message types.

E. Each service controller executing on the external processor supports a specific type of service. (Each service controller may be based on a generic controller with service-specific APIs.) The invention allows implementation of new services by the introduction of new SCs (or modification of existing SCs) without requiring changes to the PAD. Multiple service controllers provides the ability to add new services or modify existing services by the addition or replacement of service controllers rather than requiring all services to be disrupted during upgrades.

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[signature] 4/27/00	[signature] 5/01/00	[signature] 5/02/00
Print Name David E McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

SCs can be installed on multiple external processors. Additional external processors are easily added according to service requirements, which results in the good scalability.

F. The external processors provide added security against theft of services and attacks. The external processors may be maintained in a secure environment while leaving the forwarding functions of the PAD in a less-secure environment. In addition to being physically separate from the PAD, security software and/or hardware on the external processor may be implemented. TCP sessions to configure the PAD from the IP addresses other than its master external processors would be denied by the IP Filter.

G. Since the PAD intercepts network, transport and application level messages, it enables the identification of applications and users, and sets up an appropriate priority or provides the desired bandwidth to the data flows of user applications. For example, RSVP together with Microsoft subnet bandwidth manager (SBM) provides an application with guaranteed bandwidth and priority end-to end across the local and wide area networks.

H. As Internet traffic patterns change to be well-distributed around the globe, the ability to apply service and policy at the access separately from routing on a regional basis provides a more scalable design for forwarding traffic toward the distant destination.

I. The usage monitor in PAD is able to track the statistics of different layer-2 and layer-3 traffic types. When the volume of traffic for a specific type across a threshold, this event is reported to SC. The Signaling Processor within the External Processor works with the SC to ensure that active SLAs are maintained throughout the network. This coupling of the policy accessed by the SC and the dynamic SLA support in the network provides a more flexible solution that is available with today's TDM approach to SLAs.

3. Specifically describe the item and its operation. Attach copies of drawings, sketches, prints, photographs and illustrations, which should be signed, witnessed and dated. Use numbers and descriptive names in descriptions and drawings.

See attached.

4. List all known and other possible uses for the item.

PAD can be put in multiple places in the network to perform traffic management and policy control. The SCs are sized to meet the anticipated control and management traffic. The examples of the placement of PAD devices are

A. Placement of PAD devices in access networks, i.e. fiber, xDSL, cable modem, WAP, etc. connecting customer equipment to a provider network controlled by regionally located external processor running SC logic.

B. Placement of PAD devices at a provider's Point of Presence (POP) interfacing to a customer site over private line, FR, ATM, MPLS or an Ethernet access network.

C. Placement of a PAD device facing a server farm that can be in the provider's POP or in the customer sites.

5. List the features of the item that are believed to be novel.

A. The concept of the separation of the service control and switching functions applied to connectionless IP services. Previously the state of art of separated control and switching applied only to connection oriented switching.

B. By virtue of the separation of the PAD from the SC, traffic management and policy control occur much closer to the application than current network implementations achieve.

C. Independent and distributed service control of the PADs results in several novelties. Multiple SCs per PAD means that new services can be implemented rapidly and independently of other existing services. Balancing of traffic load can also be done efficiently. Also, a single SC may control multiple small PADs to reduce the overall network cost.

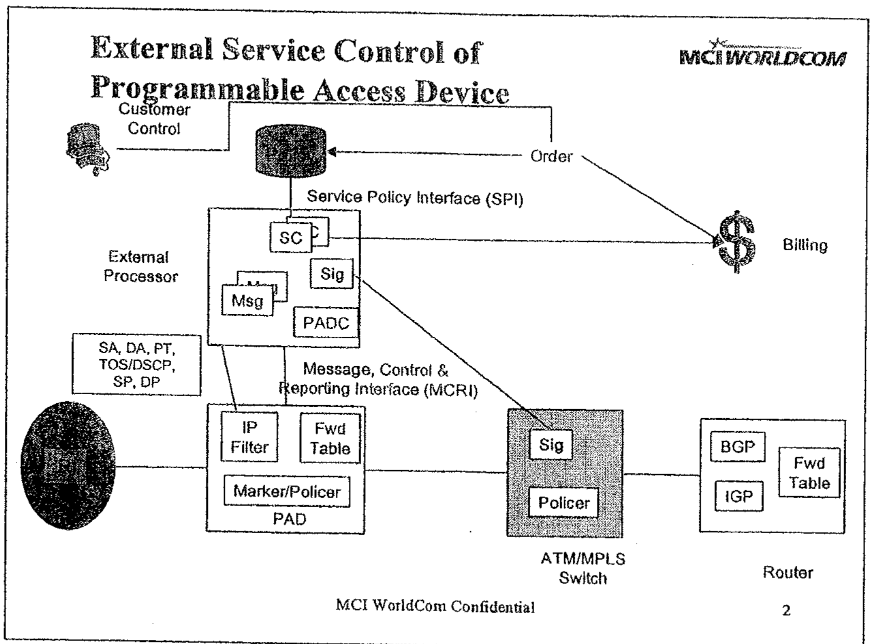
Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan 4/27/00	H. Lee Thomas 5/01/00	Lei Yao 5/02/00
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

Attach Text or Drawings:

A.1 The Concept of External Service Control of a Programmable Access Device

Figure A.1 shows the components of the Access system implementing the PAD and SC concept. The Access system includes an External Processor, a PAD and a Policy Server. The SPI (Service Policy Interface) is the interface between Policy Server and SCs. MCRI (Message Control and Reporting Interface) is the interface between SCs and PAD. Detailed descriptions of these components and interfaces are contained in this section.

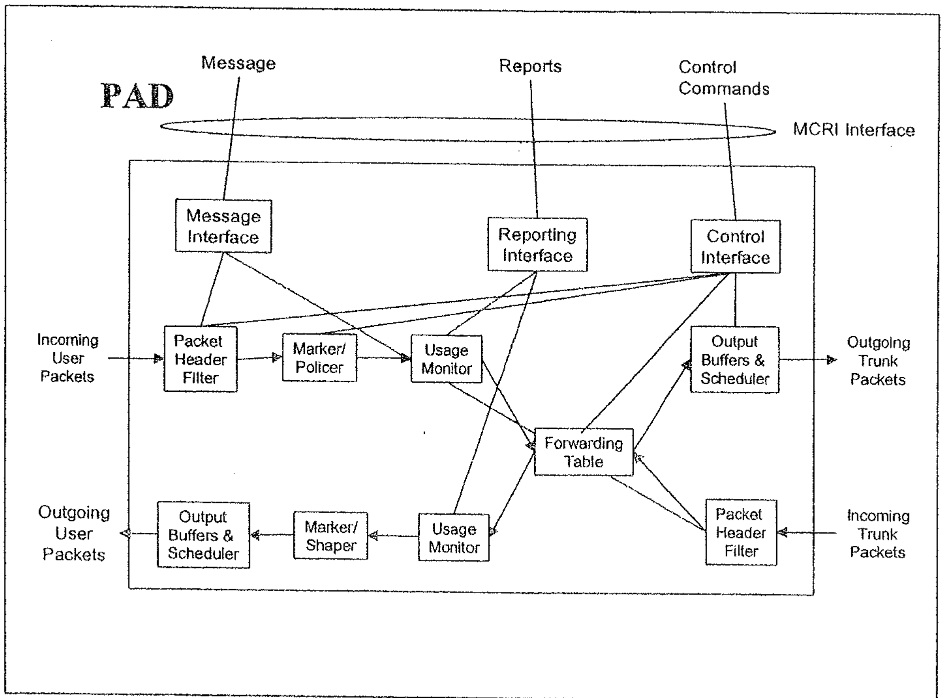
The External Processor is a general purpose computer and/or a special purpose hardware to providing environment for one or multiple SCs and interface device drivers. A service controller can be implemented either by hardware or by software. A service controller is able to interpret service-specific messages and invoke the appropriate policy control and network signaling procedure. The service controller configures the PAD using MCRI according to the policy decisions received from the Policy Server via the SPI. Separation of the SC processing from the forwarding performed in the PAD allows allocation of external processing resources to SC functions as necessary without degrading the forwarding performance of the PAD. In fact, SCs can be allocated to external processors and PADs in an arbitrary manner in response to access traffic patterns. This design is more scalable than the traditional monolithic design since the response to traffic that requires more service message processing is simply the installation of more and/or faster external processors.



(Figure A.1 External Service Control and PAD)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan 4/27/00	H. Lee Thomas 5/01/00	Lei Yao 5/02/00
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

A.2 Programmable Access Device (PAD)



(Figure A.2 PAD)

Figure A.2 shows the detailed components of the PAD. The PAD is a programmable access device with generic forwarding, marking, policing and IP filter functions. All these functions must be able to be configured or programmed by a SC through the MCRI.

The Packet Header Filter operates on the DA, SA, TOS, SP, DP and other fields of a packet received from a user device and is configured by the control interface. It either directs a packet to a specific marker/policer, or else redirects the packet to the message interface. The message interface may also inject a packet into the Packet Header Filter.

The policer applies one or more token or leaky bucket algorithms to the stream of received packets to determine conformance to traffic parameters established by the control interface. The results of the policing function can be discard of nonconforming packets, marking of nonconforming packets, or counting of nonconforming packets.

The marker function sets the bits in the DiffServ/TOS byte, and/or the 3-bit MPLS experimental field, and/or the 20-bit MPLS label field, and/or other fields for a specific flow as configured by the control interface.

The Usage monitor tracks the statistics of different layer-2 and layer-3 traffic types. Thresholds and other criteria can be set up to invoke a reporting event. The reporting messages sent to the SC may summarize the usage information for a customer, report the occurrence of a high-priority traffic flow or warn the large volume of out-of-band traffic etc.

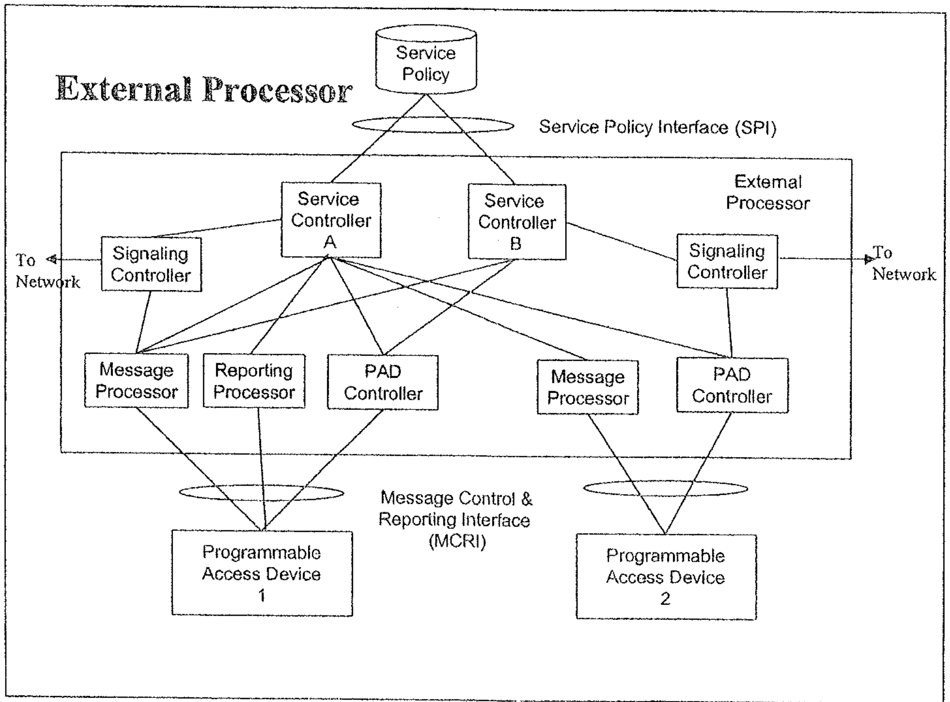
Output buffers can be a single large buffer or distributed multiple buffers. A percentage of the total buffer or a fixed amount of buffer can be assigned to a class of traffic or a traffic flow classified by DA, SA, TOS, PT, SP and DP. Packet scheduler applies Weighted Round robin and other algorithms to support statistical multiplexing. The combination of the buffering mechanism and scheduling mechanism can put a limit on the queuing delay to transmit a packet over the PAD.

The Shaper discards the nonconforming packets, sends marked packets to appropriate queues, and controls the delay jitter of a flow.

Forwarding table keeps entries for each forwarding path. A forwarding path is represented by the packet flow attributes, i.e. DA, SA, TOS, PT, SP, DP, the incoming port and the corresponding output port.

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

A.3 External Processor



(Figure A.3 External Processor)

Figure A.3 illustrates the logical elements within the External Processor. The External Processor is composed of several control and process functions that are utilized by policy servers and PADs to determine and affect the appropriate processing of packets and messages to and from customer applications.

PADs send messages, report information and control commands to the External Processor through the Message Control & Reporting Interface (MCRI). The Message Processor, Reporting Processor and PAD Controller utilize the MCRI.

The Reporting Processor and Message Processor parse messages from PADs and notify the SC of the semantics of the messages. The difference between them is that the Reporting Processor processes only the reporting messages and the Message Processor processes all the other messages. The Report Processor is able to configure the reporting functions of the PAD including the type of reporting message, the content in the reporting message, whether to pass or not pass report information, etc. The Message Processor is able to configure the IP filter to pass or not pass specific messages based on SA, DA, PT, SP, DP and/or other fields.

The PAD controller configures and manages the PAD. The PAD Controller operates on the PAD Forwarding table, IP filter, Usage Monitor, Marker/Policer/Shaper, Buffer and Scheduler by commands or scripts.

The Signaling Controller supports signaling protocols (e.g. RSVP, LDP, PNNI, FR UNI, ATM UNI, etc.) to set-up or tear down a VC or LSP across the network. The VC or LSP may have QoS specification with it.

The Service Controller (SC) is the main control module for each service. It translates the messages from the Message Processor and Reporting Processor into appropriate policy queries and sends them to the PDP. It launches VC or LSP setups across the network through the Signaling Controller. It configures forwarding table, IP filter, Marker/Policer, Shaper, buffer and scheduler on a PAD by the PAD controller. All these working together delivers the desired service for the customer traffic. The service controller should have a table recording all the active sessions. Each PAD has at least a primary and secondary SC. If a PAD loses contact with the primary SC contact will be initiated with the secondary SC. The PAD will report state information to the secondary SC. Therefore, no synchronization is required between the SCs.

To reduce the number of messages passed between a SC and the PDP, SCs are required to cache the frequently used policy lookups in its policy caches. For an incoming policy query, a SC looks up its policy caches first before it sends the query to the PDP. When a SC directly queries the PDP for a new service request, the SC may also request the PDP to dump all the related policy information from the policy database to its policy caches. Caching enables subsequent policy queries to utilize information that has already been retrieved recently from the policy server and reduce the message traffic between the SC and PDP. However there is a tradeoff between the number of direct policy queries and the cache refresh frequency and the amount of policy information downloaded from the PDP at each refresh. The objective would be to cache the

policies for IP services requiring intensive policy queries, such as SIP calls. There would be no need to cache the policy lookups for a TCP session that issues only one policy query in its lifetime.

The PDP within a policy database interacts with a SC by utilizing the Service Policy Interface (SPI). With the SPI, a SC is able to use COPS, LDAP and other policy query protocols to query the PDP within the policy database. The policy database resides on a policy server which would be an external processor resident on hardware separate from the External Controller and placed in different locations within the network. The SC sends policy requests to the PDP. The PDP returns the policy decisions for each request. The policy decision can be "approve", "reject" or configuration parameters for the SC and PAD. The PDP maintains usage information used by policy decision. For example, as a customer reserves bandwidth, the PDP needs to track the amount of bandwidth reserved by the customer and approve or reject a new service request by comparing the amount of remaining bandwidth allowed and the amount of bandwidth needed by the new service.

With open SPI and MCRI, the carrier administrator should have the full control of the SCs and programmable access devices by writing scripts or configuring parameters. Customers could also be granted limited control over the SCs and PADs in support of self-provisioning.

A.4 Interfaces

A.4.1 Service Policy Interface (SPI)

PDP to SC

- Set Inactivity Timer
- Approve the transaction
- Reject the transaction with a cause indication
- Return parameters in response of request
- Dump the policy lookups into SC policy caches

SC to PDP

- Translate Signaling Messages into appropriate Policy Queries, e.g. RSVP -> COPS (RSVP), SIP-> COPS (SIP)
- Query Policy Requirements
- Set the flag for caching of Policy lookups
- Translate Policy Decisions into appropriate control commands

A.4.2 Message, Control and Reporting Interface (MCRI)

PAD to External Processor

- Message Passing
  - Pass based upon SA, DA, PT, SP, DP, and/or other fields such as TCP Flags (SYN, ACK, RST, FIN, ...)
- Reporting
  - TCP Retransmit Threshold Crossed
  - Inactivity Timer Expired
  - Activity Detected
  - Keepalive/Heartbeat Exchange
  - State synchronization in event of SC switchover
  - Traffic Threshold Crossed
  - Usage Statistics
- Control
  - Acknowledgement of Command
  - Command Failure indication

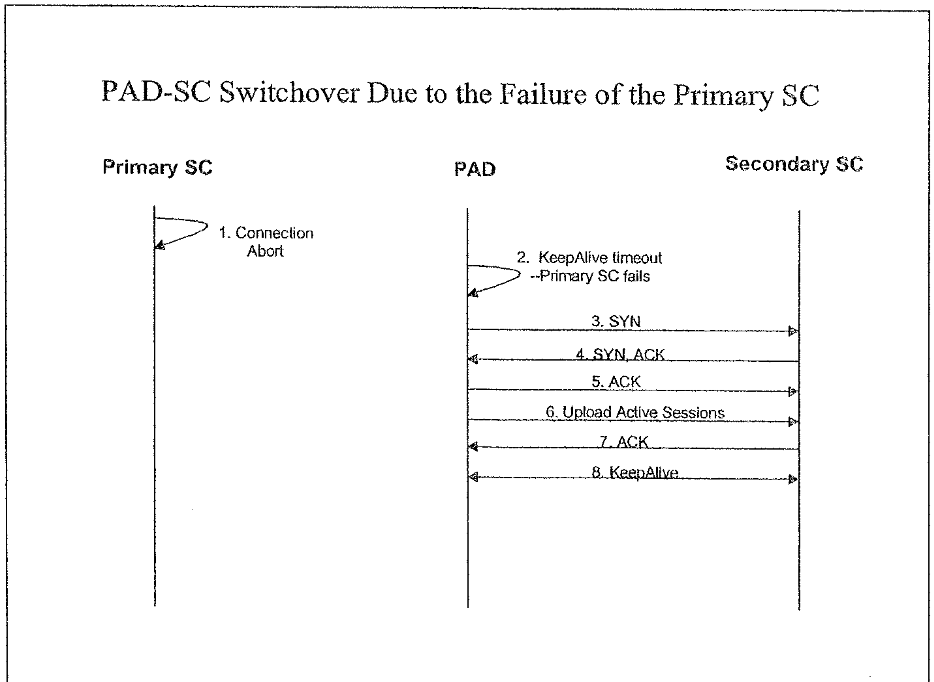
External Processor to PAD

- Message Passing
  - Inject packets into the user of trunk side interface
  - Set pass/no pass flag based upon SA, DA, PT, SP, DP, and/or other fields
- Control
  - Configure IP Filter
  - Configure Marking
  - Configure Policing
  - Configure Output buffers & Scheduler
  - Configure Shaper
  - Drop multicast packets from a source
  - Admit/Deny Source Routing Option
  - Set TCP Retransmit Reporting Threshold
  - Set Inactivity Timer
  - Set Activity Timer and Level
  - Configure Forwarding Table
  - Set Traffic Reporting Threshold
  - Allocate Resource (Bandwidth, Queue & CPU time) to a customer, a flow, a route or a multicast tree
  - Set Reporting Flags (True/False)
  - Set SVC, PVC or LSP

A.4.3 PAD-SC Switchover Operation

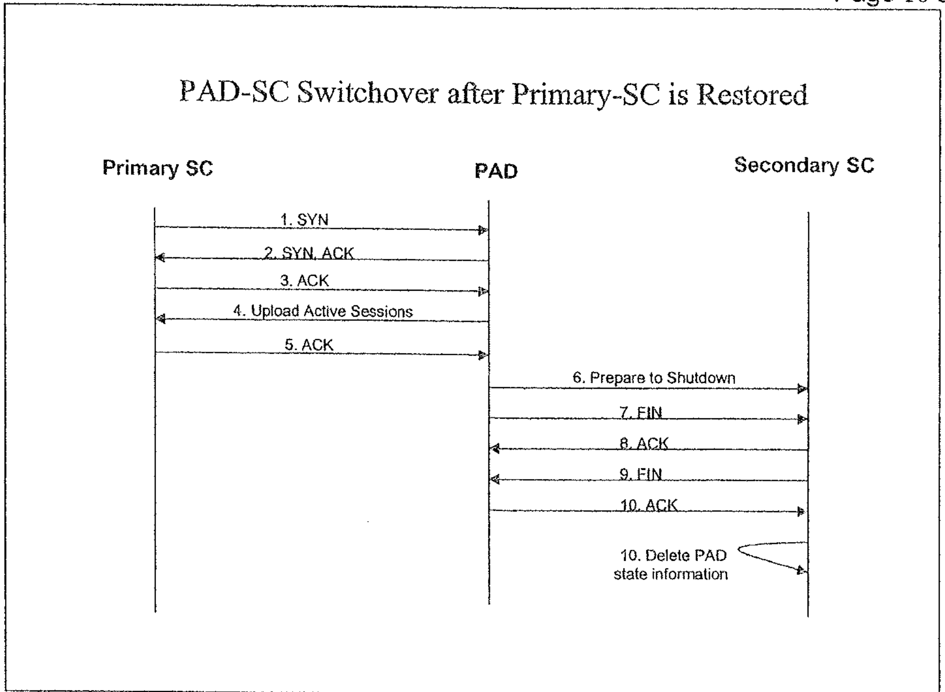
To prevent the interruption of the service, the PAD will switch to a backup SC in the event of a fault in the primary SC or the loss of connectivity to the primary SC. The PAD uses a reliable communication protocol (e.g. TCP session) to exchange information with SCs. The KeepAlive message is exchanged between the PAD and a SC periodically to keep the TCP session active. When the KeepAlive message timeouts, the PAD detects the failure of the SC. The PAD starts setting up a new TCP session with the secondary SC. If the PAD could not connect with the

secondary SC, the PAD would stop accepting new sessions and keep the state and the service for all the active sessions. After the TCP session between the PAD and the secondary SC is established, the PAD starts uploading the state information of all the active sessions controlled by the failed SC to the secondary SC. The PAD is required to keep the state machine for each active session. (See Figure A.4 The PAD successfully switches from the primary SC to the secondary SC after detecting the failure of the primary SC)



(Figure A.4 The PAD successfully switches from the primary SC to the secondary SC after detecting the failure of the primary SC)

The communication between the PAD and secondary SC may remain in a non-revertible mode, or may revert to the primary SC in a revertible mode to maintain load balancing of SC processing across the distributed PADs. Reversion to the primary SC may be accomplished with no service interruption as follows. When the primary SC begins working again, it sends TCP session set up message to the PAD. The PAD handshakes with the SC and recognizes that it is the primary SC. The PAD uploads all the active sessions to the primary SC. After the uploading is successfully completed, the PAD notifies the secondary SC that the primary SC is up and closes its TCP connection with the secondary SC. When the secondary SC gets the notice from the PAD that the primary SC is up, it closes the TCP connection with the PAD and deletes all the related state information. (See Figure A.5)



(Figure A.5 PAD Restores Connection with Primary SC)

A.5 Examples

Several examples are provided below to illustrate how various network activities may be supported by the components of the proposed invention. Generic space-time drawings are used to illustrate the sequence of messages as they are passed between the various components of the PAD, SC and network. The following terms are used frequently in the space-time drawings:

Customer Site- Represents the point at which a device or application (typically at an end-user location) where service is desired. The customer application may be requesting, for example, network resources (e.g. RSVP) or to participate in a private broadcast (e.g. multicast).

PAD- The Programmable Access Device as described is section A.2.

PDP- The Policy Decision Point is a logical point that resides within the policy server. Messages to and from the PDP are carried by the Service Policy Interface as described in sections A.3 and A.4.1.

Network- The network line in the drawings represents routers or switches within the service provider network that would that send a message or packet to an egress point or corresponding system at another access point on the network. The far end network system would process the request or packet being sent by the Customer Site or PAD.

The following examples are provided in the sections that follow:

Network-Level Signaling Example
- RSVP Signaling Example

Connection-Oriented Transport Examples Using TCP Sessions
- TCP State Machine on the PAD
- TCP Session Establishment
- TCP Session Close
- TCP Session Unauthorized
- TCP Session Timeout
- TCP Session Abrupt Close

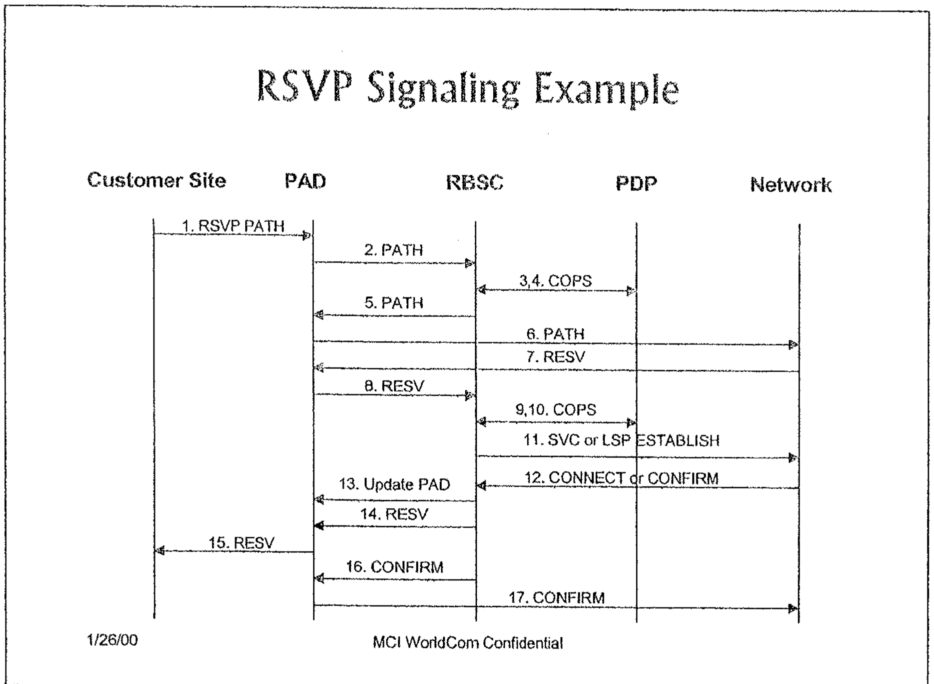
Connectionless Transport Examples Using UDP Reporting Function
- UDP Reporting Successful
- UDP Reporting Unauthorized
- UDP Reporting Timeout

Application-Level Examples Using SIP Signaling
- SIP Call Establishment
- SIP Call Termination
- SIP Call Timeout
- SIP Call Negotiation

IP Multicast Examples
- Authorized Registration of a New Multicast Group
- Unauthorized Registration of a New Multicast Group
- Authorized Membership Query
- Unauthorized Membership Query
- Authorized Sending of Multicast Packets
- Unauthorized Sending of Multicast Packets
- Receiving Authorized Multicast Packets
- Receiving Unauthorized Multicast Packets

A.5.1 Network-level Signaling Example

In the example shown in Figure A.6, the customer application initiates an RSVP PATH message (1). The PAD forwards the PATH (2) message to the SC, which is called a Reserved Bandwidth Service Controller (RBSC) in this example. The RBSC queries the PDP (3). The PDP approves the RBS to the customer (4). The RBSC returns PATH (5) to PAD. PAD sends the PATH (6) message downstream to the other end of the network. The receiver responds by a reservation (RESV) message (7). The PAD passes the RESV (8) to the RBSC, which invokes another policy query (9). The PDP approves and records the bandwidth requirements by the RESV (10). (Here we assume that the PDP keeps track of the allocated bandwidth for a customer. The occupied bandwidth is compared with the committed bandwidth to a customer for policy-based admission decision.) The RBSC then kicks off either the ATM signaling or the MPLS signaling to set up a SVC or a LSP (11). After the connection is confirmed (12), the RBSC configures the PAD's IP filter and forwarding table to transmit packets of this flow over the established SVC or LSP (13). The RBSC in turn returns RESV (14) to the PAD. The PAD sends the RESV (15) upstream to the sender application. The RBSC also sends the CONFIRM downstream to the receiver (17) to finish the handshake for setting the SVC or the LSP. In this example, the IP filter in PAD captures RSVP messages according to its protocol type (PT=46).

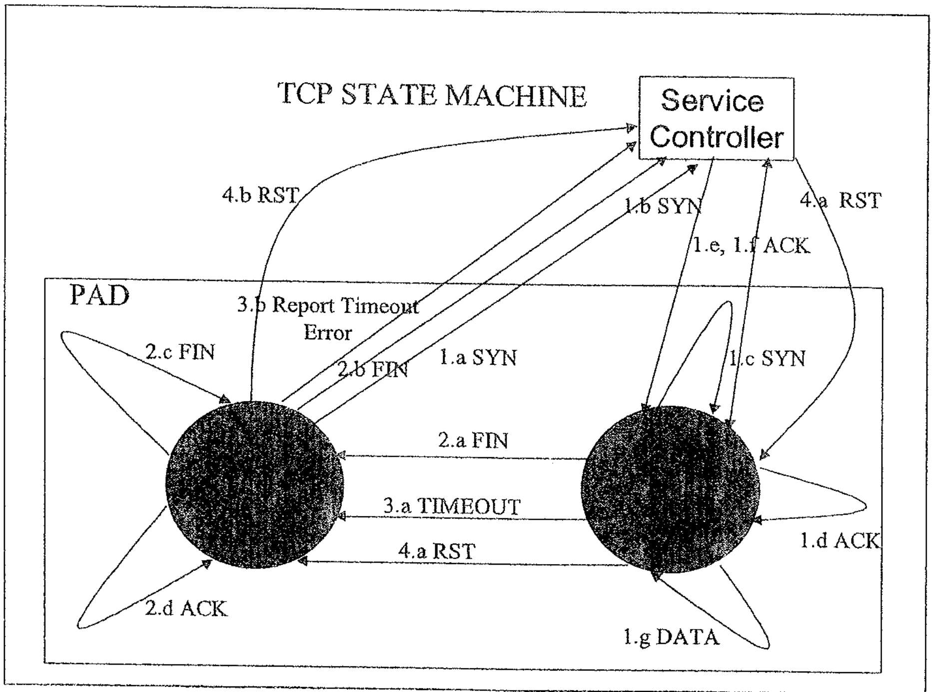


(Figure A.6 RSVP Signaling Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

A.5.2 Connection-oriented transport examples using TCP sessions:

- TCP State Machine on the PAD



(Figure A.7 TCP State Machine)

The TCP state machine on the PAD has two states: idle and active. The state transition is described below:

IDLE -> ACTIVE

1. When the state machine is in the idle state (non-existing TCP session), it passes and only passes the first SYN message received from the user to the SC (1.a). The SC queries the policy server for policy decisions for this TCP session after it receives the SYN message from the PAD. If the TCP session is approved, the SC returns the SYN message back to the PAD (1.b). The PAD changes the state machine to the active state and forwards the SYN message to the receiver to complete the three-way handshake (1.c, 1.d). The PAD passes the ACK message representing the success of the handshake to the SC (1.e). The SC knows the TCP session is open and adds the TCP session into its active session table. The SC updates the PAD with an inactive timer and other related parameters of this TCP session and then sends the ACK back to the PAD (1.f). The TCP session is ready for data transmission (1.g).

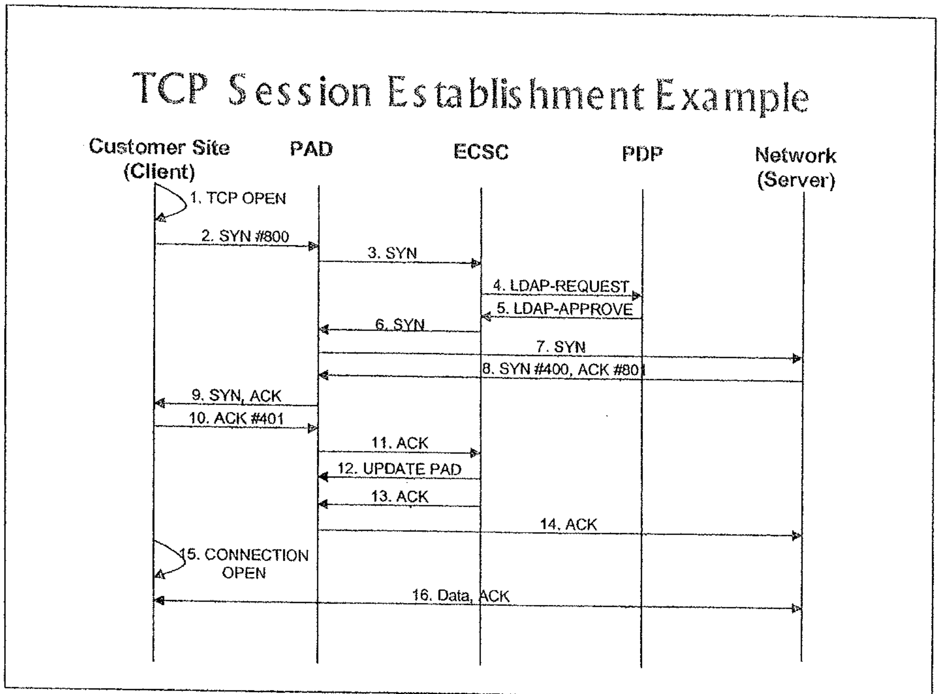
ACTIVE->IDLE

2. When the PAD receives a FIN message from the either side of a TCP connection for an active TCP session, it resets the TCP state machine to be idle (2.a). The PAD passes the FIN message to the SC (2.b). The SC learns that the TCP connection is inactive and deletes the TCP session from its active session table. The PAD forwards the FIN message to its destination to complete the three-way handshake for closing the TCP connection (2.c, 2.d). The PAD deletes the state machine of the TCP session.
3. When the inactive timer on the PAD for an active TCP session expires, the PAD resets the TCP session to be idle (3.a). The PAD reports the timeout error to the SC (3.b). The SC deletes the TCP session form its active session table and updates the PAD. The PAD deletes the state machine of the TCP session.
4. When the PAD receives a RST segment from either side of a TCP connection, it knows that an abrupt close is requested and resets the TCP session to be idle (3.a). The PAD reports the timeout error to the SC (3.b). The SC deletes the TCP session from its active session table and updates the PAD. The PAD deletes the state machine of the TCP session.

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[signature] 4/27/00	[signature] 5/01/00	[signature] 5/02/00
Print Name David E. McDysan	Print Name H Lee Thomas	Print Name LEI YAO

- TCP Session Establishment

SCs configure the PAD to pass TCP SYN messages for non-existing TCP sessions to them. In the example shown in Figure A.8, The client application issues an OPEN (1) command that tells TCP that it wants to open a connection to a server at a given port and IP address. The client TCP picks an initial sequence number (800 in this example). The client TCP sends a synchronize segment (SYN) carrying this sequence number (2). When the SYN arrives, the PAD detects that it is a mission-critical e-commerce TCP session based on the destination IP address and port number (PT=6, PORT=80). The PAD passes the SYN to the e-commerce service controller (ECSC) (3). The ECSC asks for the policy and admission control from the PDP (4) using LDAP or some other policy query protocol. The PDP approves the TCP session (5). The ECSC sends the SYN back to the PAD (6). When the PAD receives the SYN from the ECSC, it spawns a new TCP state machine and sets it to an active state (7). The PAD sends the SYN downstream to the server (7). When the SYN arrives, the server TCP picks its initial sequence number (400 in this case). The server TCP sends a SYN segment containing initial sequence number 400 and an ACK of 801(8), meaning that the first data byte sent by the client should be numbered 801. The SYN/ACK message is sent back to the client (9). When the client TCP receives the server's SYN/ACK message, the client TCP returns an ACK of 401 (10), which means that the first data byte sent by the server should be numbered 401. The PAD passes the ACK to the ECSC (11). The ECSC learns that the three-way handshake is successful and the TCP session is open. The ECSC adds the TCP session into its active session table and configures the PAD (12) with the number of retransmissions and the inactive timer. The ECSC also sets the marker to mark the packets belonging to this TCP session as high priority. (For some applications, such as the training applications that will only allow the teacher to disconnect the TCP sessions, the SC configures the IP Filter to ignore the client FIN.) The ECSC then returns the ACK segment to the PAD (13). The PAD sends the ACK to the destination server (14). The client TCP notifies its upper layer application that the connection is open (15). The client and the server start exchanging data in the TCP session (16).

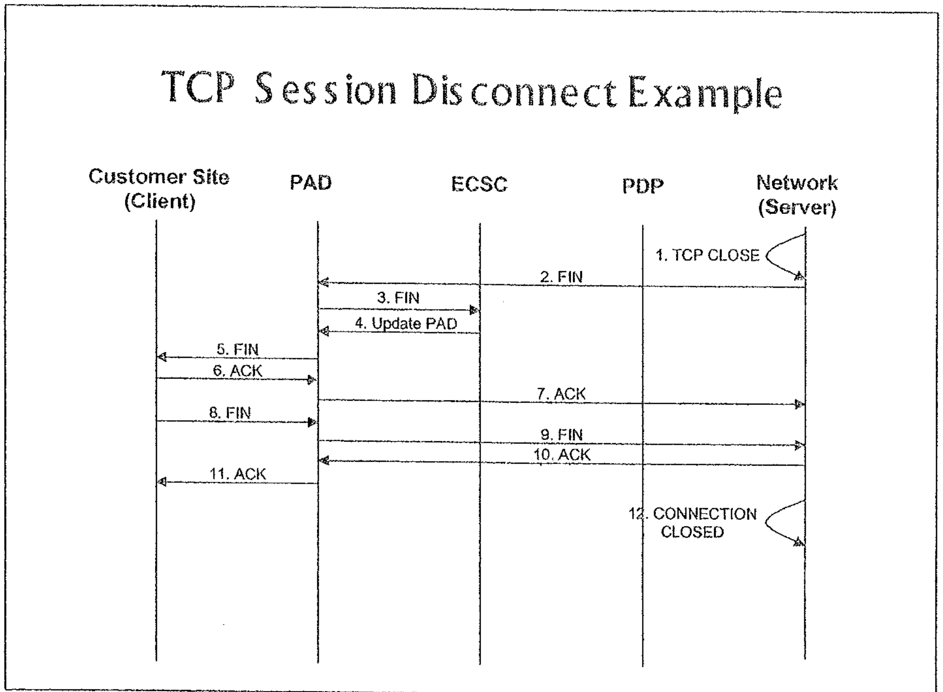


(Figure A.8 TCP Session Establishment Example)

Inventor Signature / Date	Inventor Signature / Date	Inventor Signature / Date
David E. McDysan 4/27/00	H. Lee Thomas 5/01/00	Lei Yao 5/02/00
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

- TCP Session Close

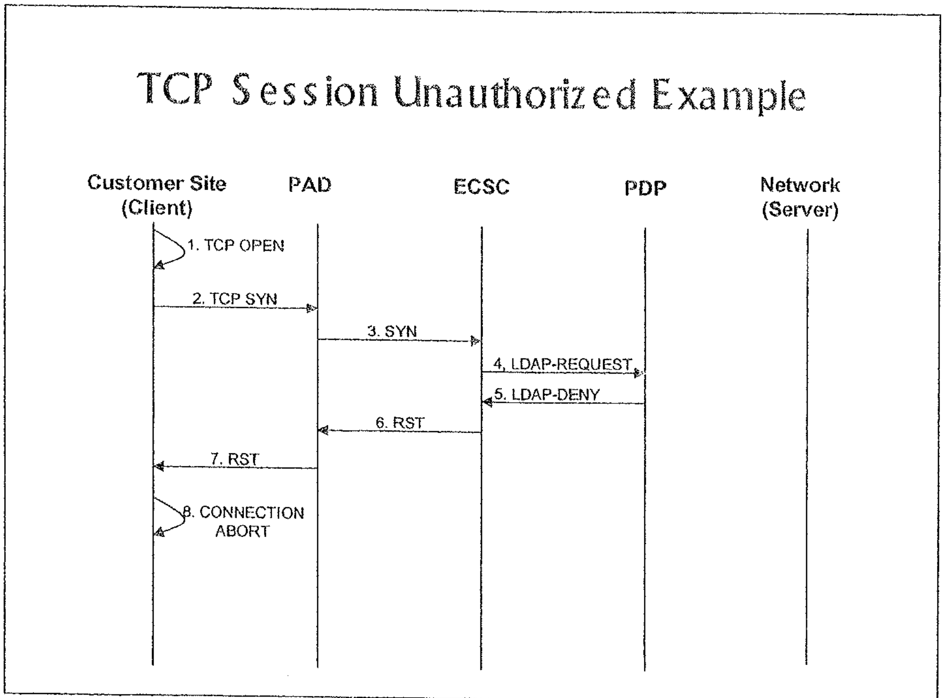
Either side of a TCP connection can launch a close. The server initiates the close in the example shown in Figure A.9. The server application has finished its work and tells TCP to close the connection (1). The server TCP sends a FIN segment (2), informing the partner that it will send no more data. The PAD resets the state machine of the TCP connection to be idle and passes the FIN segment to the ECSC (3). The ECSC deletes the TCP session from its active session table and configures the PAD to stop marking packets for this TCP session (4). The PAD forwards the FIN segment to the client (5). The client TCP acknowledges receipt of the FIN segment (6, 7). The client TCP notifies its application that the client wishes to close. The client application tells its TCP to close. The client TCP sends a FIN message to the server TCP (8,9). The server TCP receives the client's FIN and responds with an ACK to the client (10). The PAD knows the three-way handshake for closing the TCP session is successful and deletes the state machine of this TCP session. The PAD then forwards the ACK to the client (11). The server TCP notifies its application that the connection is closed (13).



(Figure A.9 TCP Session Close Example)

- TCP Session Unauthorized

In the example shown in Figure A.10, the client application issues an OPEN (1) command that tells TCP that it wants to open a connection to a server at a given port and IP address. The client TCP picks an initial sequence number. The client TCP sends a synchronize segment (SYN) carrying this sequence number (2). When the SYN segment arrives, the PAD detects that it is a mission-critical e-commerce TCP session based on the destination IP address and port number (PT=6, PORT=80). The PAD passes the SYN segment to the ECSC (3). The ECSC asks for the policy and admission control from the PDP (4) by LDAP. The PDP denies the TCP session either because there is not enough resources in the network or because the client has not ordered the e-commerce service (5). The ECSC in turn issues a reset segment to the PAD (6). The PAD sends the RST segment upstream to the client TCP (7). When the client TCP receives the RST, the client TCP aborts the session. (Note: Since the PAD does not receive a SYN segment from the ECSC, no state machine has been created for the TCP session in this example.)

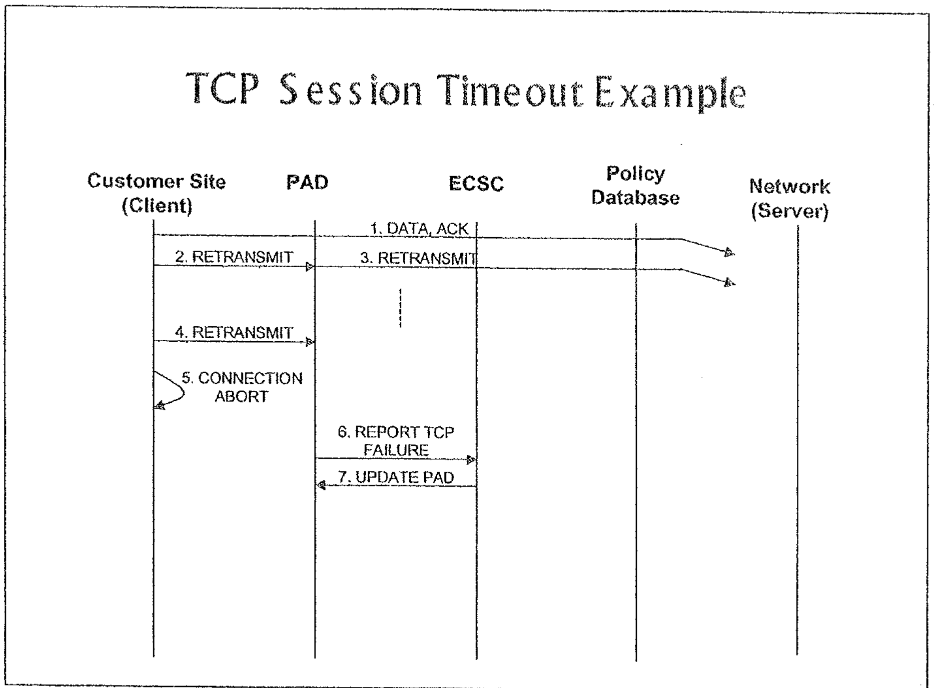


(Figure A.10 TCP Session Unauthorized Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	4/27/00	M. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name M. Lee Thomas		Print Name LEI YAO	

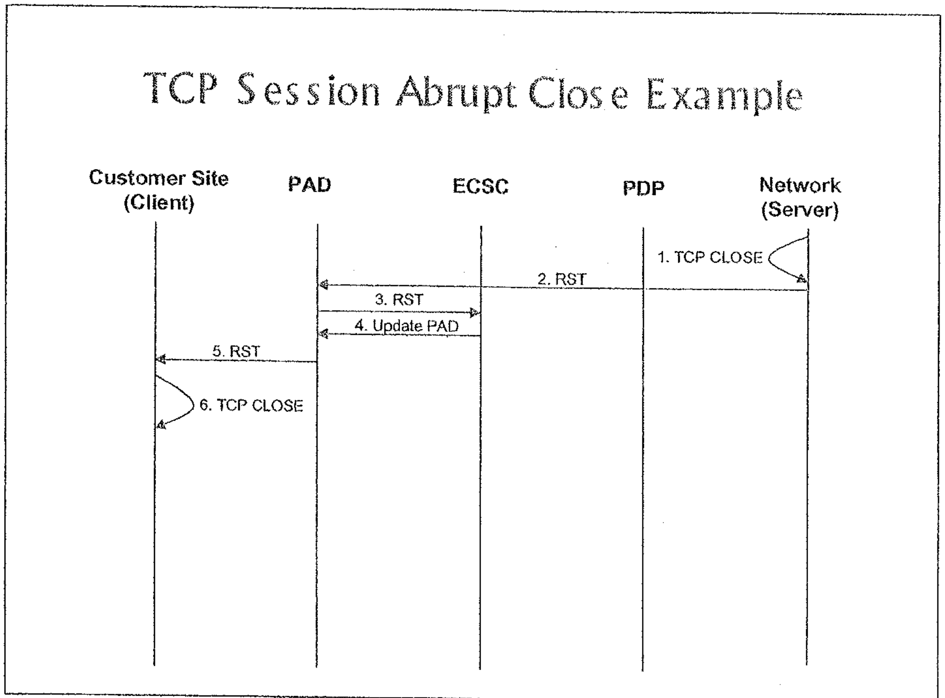
- TCP Session Timeout

Normally, TCP sessions have a proper disconnect. However, in the event a server fails or reboots or the network breaks, the TCP session is going to timeout in the host. In this case, normal disconnect will not occur. Other means must be used to update the ECSC to the inactive state for this session. In the example shown in Figure A.11, the route to the TCP partner is disrupted by loss of a link or a node (1). The client TCP starts re-transmitting the same data. After reaching a threshold number of retransmissions (2,3,4), the client TCP timeouts and aborts the connection (5). Subsequently, the inactive timer in the PAD expires. The PAD updates the TCP session to an inactive state and reports the TCP session timeout error to the ECSC (7). The ECSC deletes the TCP session from its active session table and configures the PAD to stop marking the packets for the TCP session. The PAD deletes the state machine of the TCP session.



(Figure A.11 TCP Session Timeout Example)

- TCP Session Abrupt Close
  Either side of a TCP connection can launch an abrupt close. This may be done because the application wishes to abort the connection, or because TCP has detected a serious communication problem that can not be resolved. An abrupt close is signaled by sending a RST segment to the partner. The server initiates the abrupt close in the example shown in Figure A.12 (1,2). The PAD resets the state machine for the TCP session to be idle and passes the RST segment to the ECSC (3). The ECSC deletes the TCP session from its active session table and configures the PAD to stop marking packets for this TCP session (4). The PAD deletes the state machine of the TCP session and forwards the RST segment to the client (5). The client closes the TCP session upon receiving the RST segment (6).



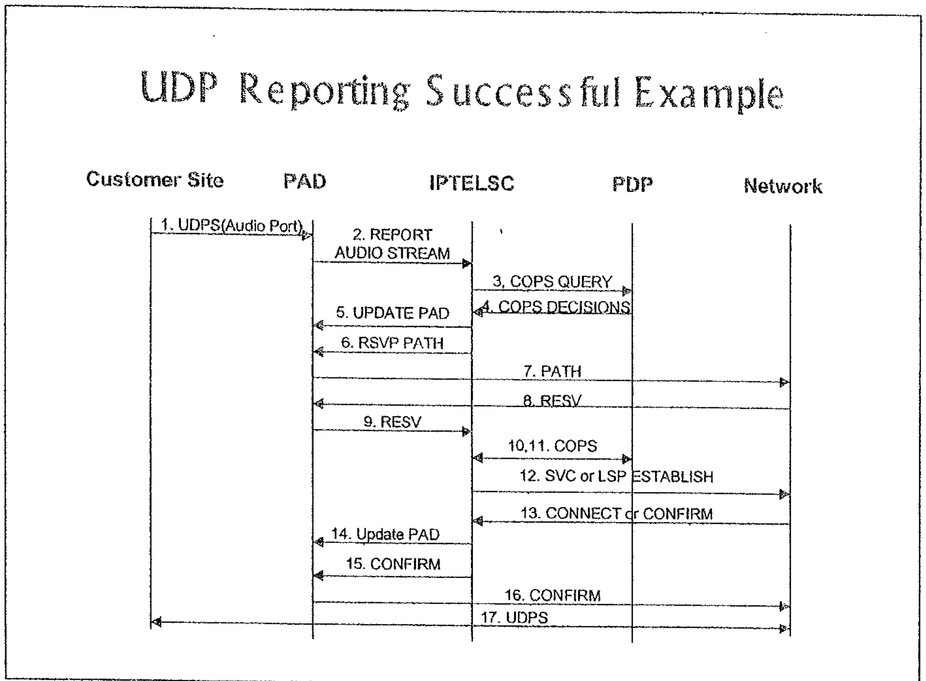
(Figure A.12 TCP Session Abrupt Close Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	05/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

A.5.3 Connection-less transport examples using UDP reporting function with specific port number ranges

- UDP Reporting Successful

  Section A.5.1 gives an example of RSVP signaling where the customer initiates the RSVP messaging. In the example shown below in Figure A.13, the client computer in the customer site does not support RSVP. A user on the customer site invokes a client program to make an IP telephone call. The client process gets an unused UDP port from the pool of available ports assigned for voice data transmission. The client application starts sending voice data encapsulated by UDP packets over the network as best-effort traffic (1). The PAD detects the constant flow of UDP packets (PT=17) within the voice port range and reports the occurrence of voice data flow to the IP Telephony Service Controller (IPTELSC) (2). The IPTELSC queries the PDP for policy decision (3) using COPS or some other policy query protocol. The PDP finds that the customer ordered guaranteed service for his IPTEL calls and commands the IPTELSC to provide guaranteed service for this IPTEL session (4). The IPTELSC configures the PAD with an inactive timer for this IPTEL call and instructs the PAD to stop reporting the occurrence of this IPTEL session. The IPTELSC initiates a reserved bandwidth route setup process (6-16). For an ATM core, a bi-directional SVC is set up. For an MPLS core, two uni-directional LSPs are set up. After the QoS path is established, all the voice UDP packets belonging to the IPTEL session are transmitted through the same QoS path (17). The PAD will periodically generate RSVP refresh messages on behalf of the user. If the IPTELSC caches enough policy information on making admission control decision in the first search (3,4), the IPTELSC does not need to query PDP for the second time and 10,11 are optional.

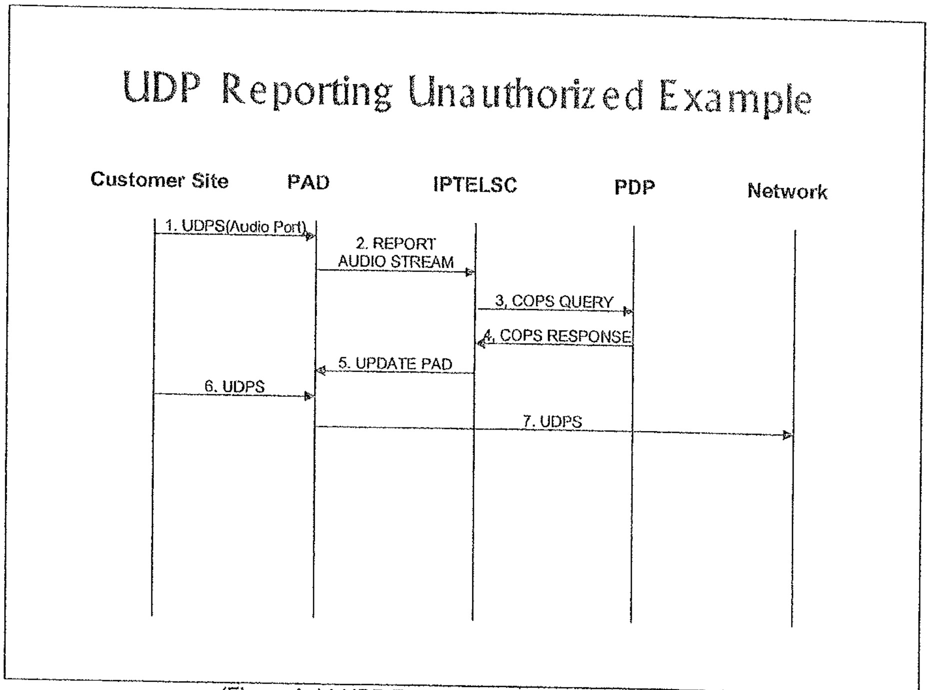


(Figure A.13 UDP Reporting Successful Example)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
David E. McDysan 4/27/00	H. Lee Thomas 5/01/00	Lei Yao 5/02/00
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

- UDP Reporting Unauthorized

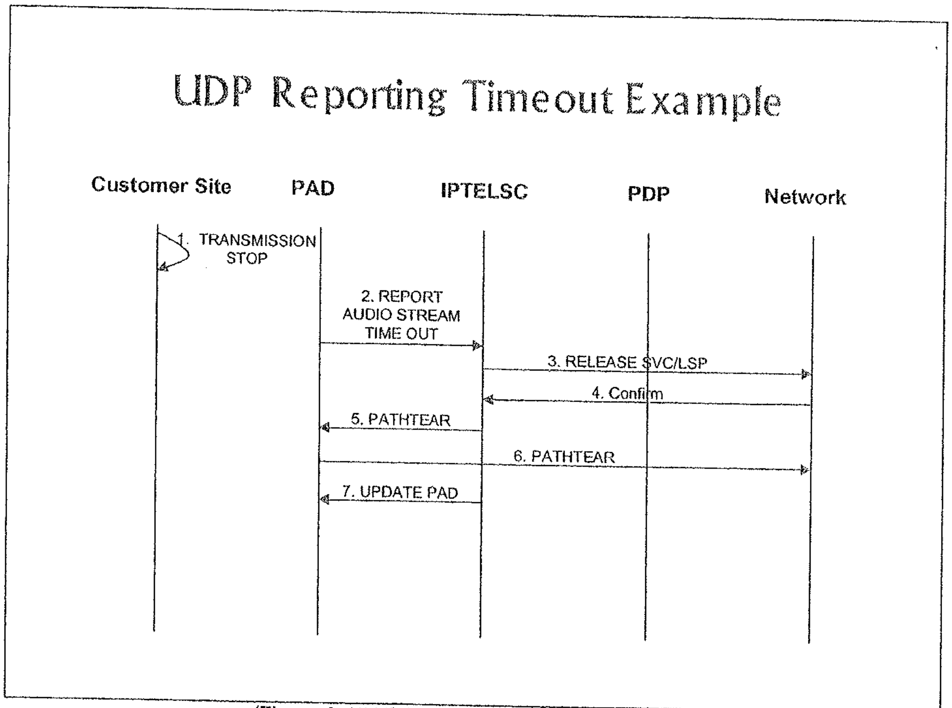
In the example shown in Figure A.14, a user on a customer site invokes a client program to make an IP telephone call. The client process gets an unused UDP port from the pool of available ports assigned for voice data transmission. The client application starts sending voice data encapsulated by UDP packets over the network as best-effort traffic (1). The PAD detects the constant flow of UDP packets within the voice port range and reports the occurrence of voice data flow to the IP Telephony Service Controller (IPTELSC) (2). The IPTELSC queries PDP for policy decision (3) with COPS or some other policy query protocol. The PDP finds that there are no QoS requirements for this customer's IPTEL calls and sends only information response back to the IPTELSC (4). The IPTELSC configures the PAD to prevent the PAD from reporting the IPTEL call again and sets an inactive timer for this IPTEL call (When the inactive timer expires, the configuration the IPTELSC made on the PAD is cleaned.) The UPD packets are sent as best-effort traffic (6,7).



(Figure A.14 UDP Reporting Unauthorized Example)

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[signature] 4/27/00	[signature] 5/01/00	[signature] 5/02/00
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO

- UDP Reporting Timeout
  The UDP session inactive timer expiry can be caused either by normal completion of the UDP data flow, the break of the transmission links, or failure of the end computers. In the example shown in Figure A.15, the client application on the customer site has finished the call and stops sending voice traffic (1). The inactive timer for the IPTEL call expires after a while. The PAD detects the timeout event and reports it to the IPTELSC (2). The IPTELSC releases the SVC or LSPs for this call (3,4) and invokes the PATHTEAR to explicitly tear down the QoS path for the call (5,6). The IPTELSC then deletes this IPTEL call from its active session table. The IPTELSC configures the PAD to delete all the configured parameters for this call.



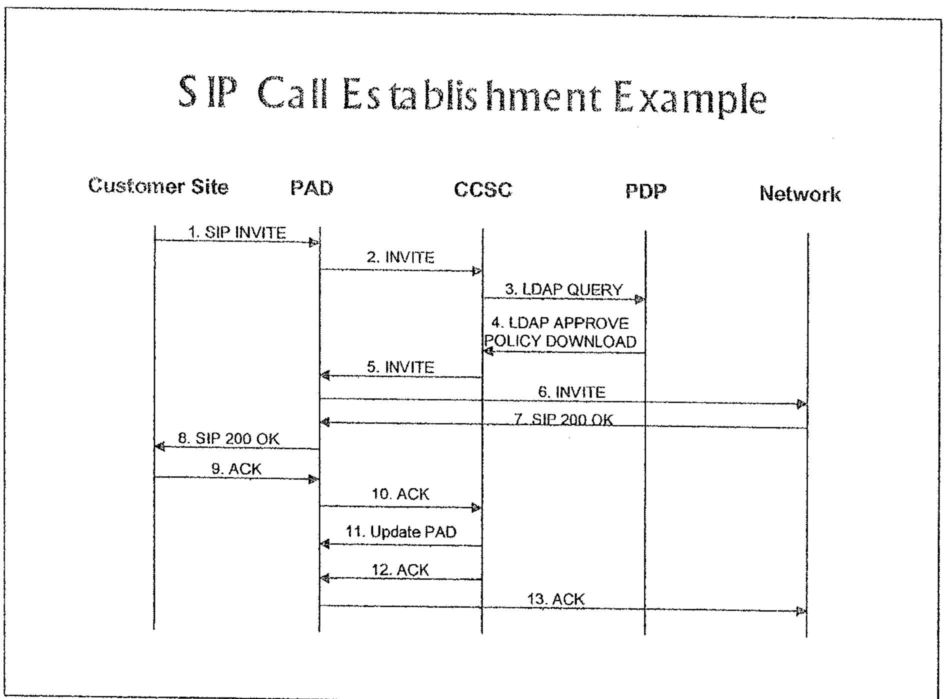
(Figure A.15 UDP Reporting Timeout Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

A.5.4 Application-level examples using SIP signaling

For SIP signaling, the PAD is required to pass almost every SIP messages to the SC because each SIP message may request a different capability set for the SIP call. Therefore, each SIP message invokes a policy query to approve a capability set. To reduce the number of messages exchanged between the SC and the PDP, the SC requests the PDP to dump the policy lookups for the SIP requester into its policy caches in its first policy query for a SIP call. The SC then uses the cached policies to make decisions for the SIP messages. The SIP state machine resides on the PAD. Thus the PAD is able to decide whether it needs to pass the received SIP message to the SC and should try to avoid forwarding SIP messages to the SC whenever possible.

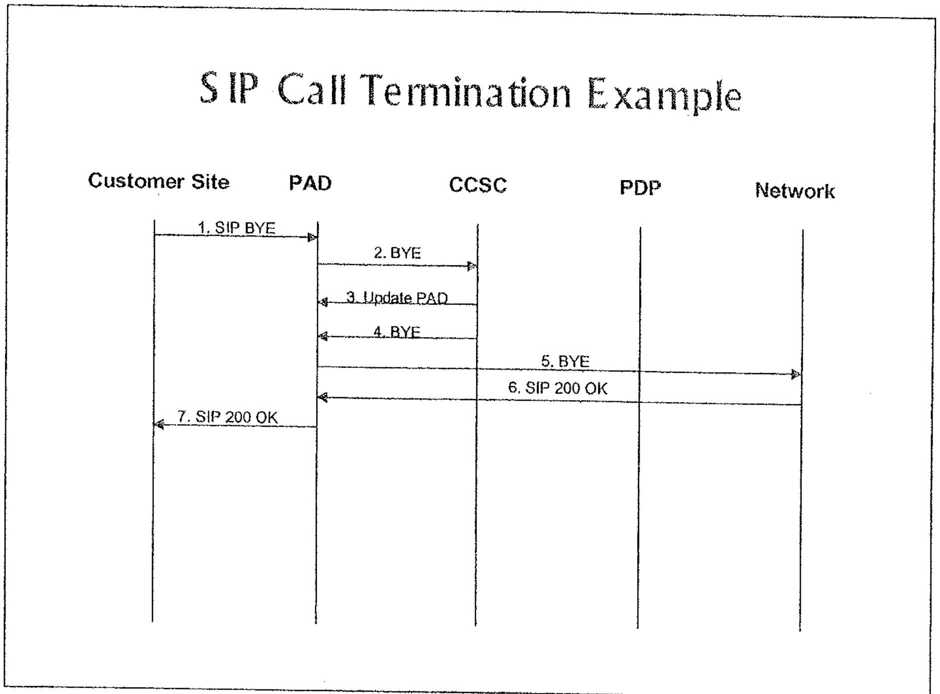
- SIP Call Establishment
  In the example shown in Figure A.16, a caller on a customer site issues a SIP INVITE request to the callee (1). When the PAD detects the INVITE request (according to the UDP/TCP port range that is assigned to SIP), it passes the INVITE request to the Conference Call Service Controller (CCSC) (2). The CCSC sets the policy dump flag and queries the PDP for policy decisions using LDAP or some other policy query protocol (3). The PDP approves the SIP session (4) and dumps the policy lookups for the SIP caller into the policy caches of the CCSC. The CCSC returns the INVITE request to the PAD (5). The PAD forwards the INVITE request to the callee (6). The callee responds to the caller via 200 OK message (7). Since there is no change in the SIP capability set the PAD forwards the SIP 200 OK message directly to the caller (8) and does not pass it to the CCSC. The caller acknowledges the acceptance of the 200 OK message via an ACK request (9). The PAD passes the ACK request to the CCSC (10). The CCSC queries its policy caches and approves the final capability set of the SIP call. The CCSC adds the SIP session into its active session table and configures the PAD with an inactive timer and other parameters to facilitate the SIP call (11). The ACK is sent back to the PAD (12). The PAD in turn sends the ACK to the callee (13).



(Figure A.16 SIP Call Establishment Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
[signature]	4/27/00	[signature]	5/01/00	[signature]	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

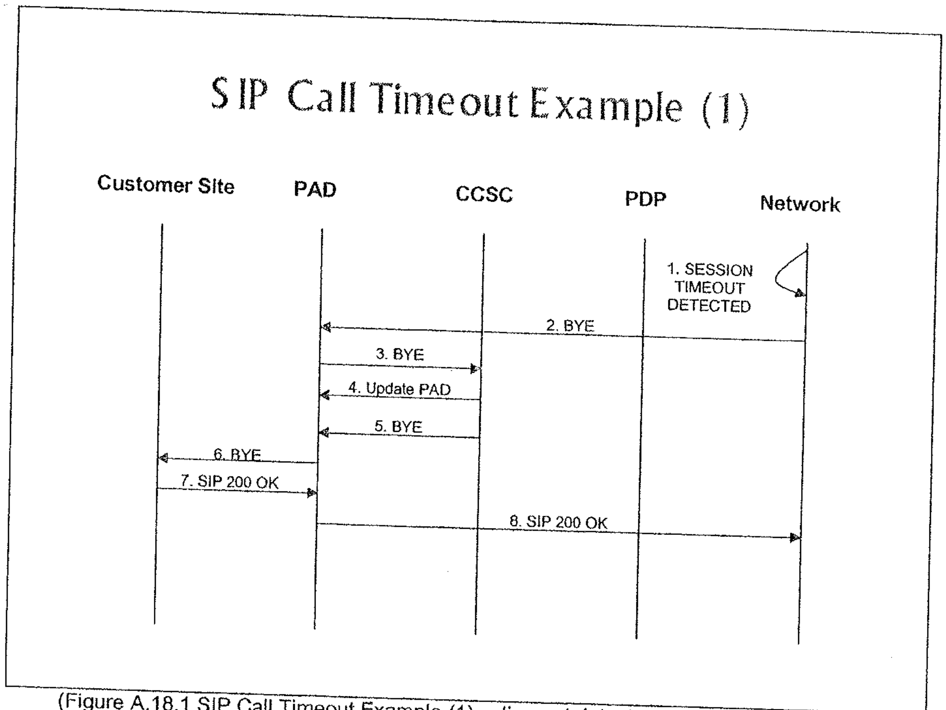
- SIP Call Termination
  In a multi-party SIP conference call, each party can only drop himself from the call. After the last party leaves the call, the call is terminated. However, in a two-party SIP call, either the caller or the callee can terminate the call. Figure A.17 shows a two-party call termination example. The caller in the customer site signals the call termination by sending a BYE request (1). The PAD passes the BYE request to the CCSC (2). The CCSC deletes the SIP session from its active session table and cleans its policy caches. The CCSC then updates PAD to delete the entire configuration for the SIP call (3). The CCSC also prevents the PAD from passing subsequent SIP messages from the SIP call. The CCSC sends the BYE message back to the PAD (4). The PAD forwards the BYE message to the callee (5). The callee acknowledges the end of the SIP call via a SIP 200 OK message (6). The PAD forwards the 200 OK message to the caller without passing it to the CCSC (7).



(Figure A.17 SIP Call Termination Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

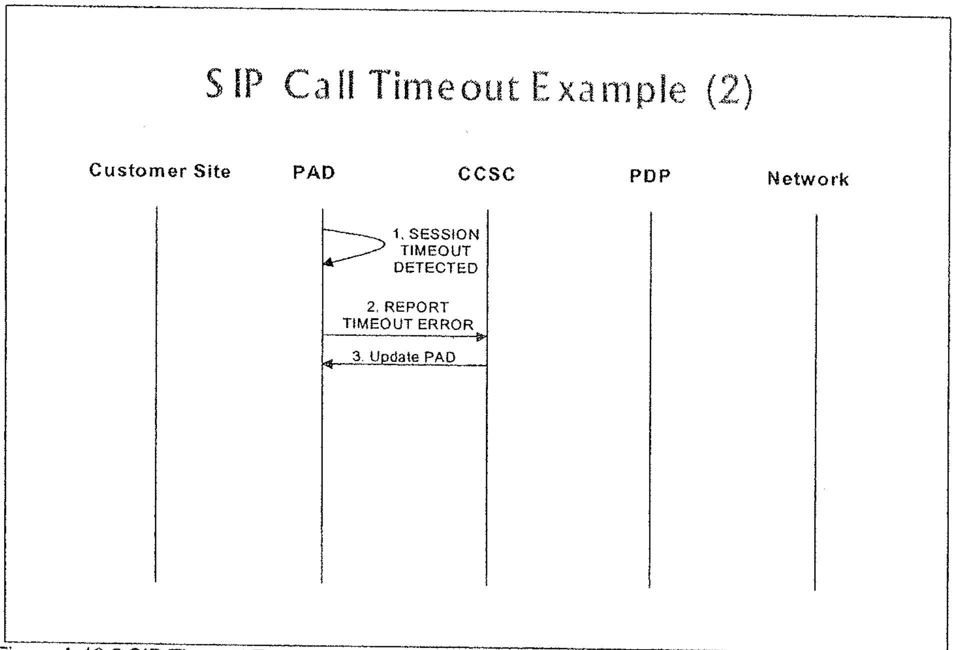
- SIP Call Timeout
  (1) In a SIP message, the ExpireTimer denotes the duration of the call before it expires. In the example shown in Figure A.18.1, the callee SIP application detects that the call has exceeded the allowed duration in ExpireTimer (1). The callee then issues a BYE request (2). The PAD passes the BYE request to the CCSC (3). The CCSC deletes the SIP session from its active session table and cleans its policy caches. The CCSC commands the PAD to delete the entire configuration for the SIP call (4). The CCSC also prevents the PAD from passing it subsequent SIP messages from the SIP call. The CCSC returns the BYE request to the PAD (5). The PAD forwards the BYE request to the caller (6). The caller acknowledges the end of the SIP session via a SIP 200 OK message (7). The PAD forwards the OK message to the callee (8).



(Figure A.18.1 SIP Call Timeout Example (1)--- timeout detected by the SIP application)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

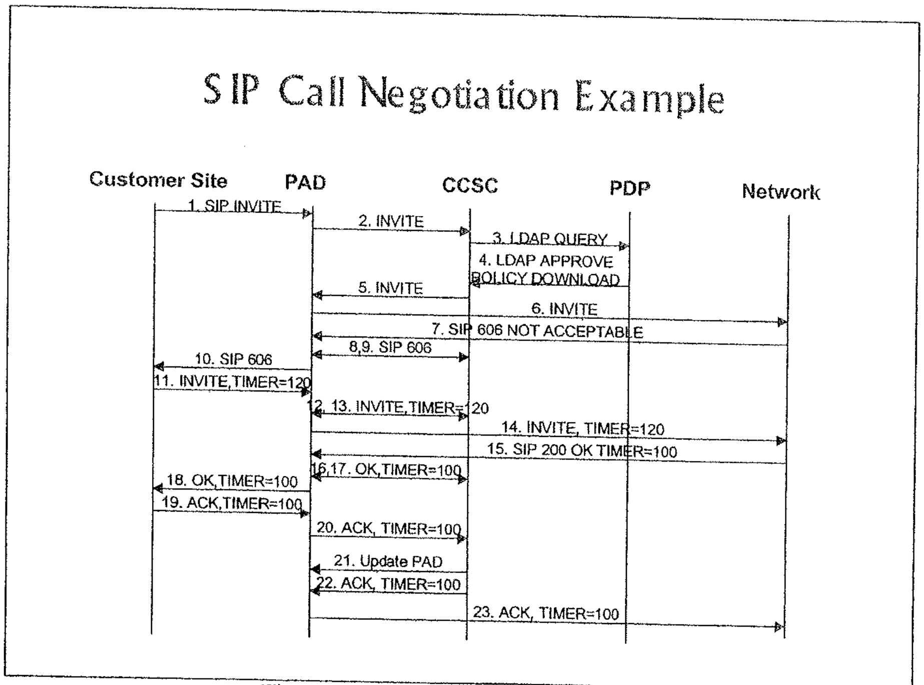
(2) In the example shown in Figure A.18.2, all parties of the SIP call die. The inactive timer of the SIP call expires (1). The PAD reports the timeout error to the CCSC (2). The CCSC deletes the SIP session from its active session table and cleans its policy caches. The CCSC commands the PAD to delete the entire configuration for the SIP call (3).



(Figure A.18.2 SIP Timeout Example (2)--- All parties in the SIP call die and timeout is detected by PAD)

- SIP call negotiation

In the example shown in Figure A.19, a caller on a customer site issues a SIP INVITE request to the callee (1). The PAD passes the INVITE request to the CCSC (2). The CCSC sets the dump policy flag and queries the PDP (3) with LDAP or some other policy query protocol. The PDP approves the SIP session and dumps policy lookups for the SIP call into the policy caches of the CCSC (4). The CCSC returns the INVITE request to the PAD (5). The PAD sends the INVITE request to the callee (6). Since the INVITE request specifies a bandwidth that is higher than what can be supported by the access link of the callee and requests a set of media encodings, the callee responds with a 606 Not Acceptable message (7). The response states that only 56 Kbps is available and that only PCM or LPC audio could be supported in order of preference. When the 606 response is passed to the CCSC (8), the CCSC queries its local policy caches and approves the new capability set. The CCSC sends the 606 response back to the PAD (9). The PAD forwards the 606 response to the caller (10). When the caller receives the 606 response, it adjusts the call capability requirements and issues another INVITE request (11), which specifies 56 Kbps bandwidth, LPC audio encoding and the ExpireTimer 120 minutes. The PAD passes the new INVITE request to the CCSC (12). The CCSC queries its local policy caches and approves the new SIP capability set again. The CCSC returns the INVITE request to the PAD (13). The PAD sends the INVITE request to the callee (14). The callee is able to support all the call requirements except that it requires the call duration to be 100 minutes. The callee responds a 200 OK response with the ExpireTimer 100 minutes (15). The PAD passes the OK response to the CCSC (16). The CCSC checks the SIP capability set carried in the OK response and approves it. The CCSC then sends back the OK response to the PAD (17). The PAD forwards the OK response to the caller (18). When the caller receives the OK response it modifies its ExpireTimer requirement to be 100 minutes and acknowledges via an ACK request (19). The PAD passes the ACK response to the CCSC (20). The CCSC approves the final SIP capability set carried in the ACK response. The CCSC configures the PAD with an inactive timer and other parameters to facilitate the SIP call (21). The CCSC then returns the ACK to the PAD. The PAD forwards the ACK to the callee. After the callee receives the ACK response, the SIP call is successfully established.



(Figure A.19 SIP Call Negotiation Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

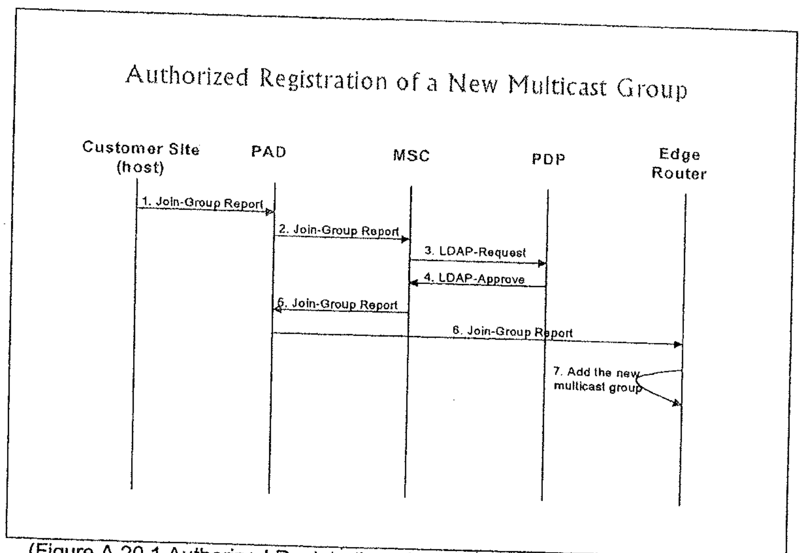
A.5.5 IP Multicast Examples

The current IP multicast uses an open group model. Sources only need to know a multicast address. They do not need to know group membership and they do not need to be a member of the multicast group to which they are sending multicast packets. Multicast group members can join or leave a multicast group at will. There is no need to register, synchronize, or negotiate with a centralized group management entity. However for a multicast service, the customers expect control and management of group membership for both the sender and receiver. For senders it is important that only authorized sources send to a multicast group. This is because either a content provider wishes to be the only source of data being sent to the group or because of concerns about denial-of-service attacks via flooding. Likewise, the set of receivers of the group must be controlled. This is because sources may wish to authorize receivers as in video distribution and video conferencing.

The proposed access system architecture in this petition enables policy-based multicast service management by monitoring the IGMP messages.

- Manage the registration of the new multicast groups

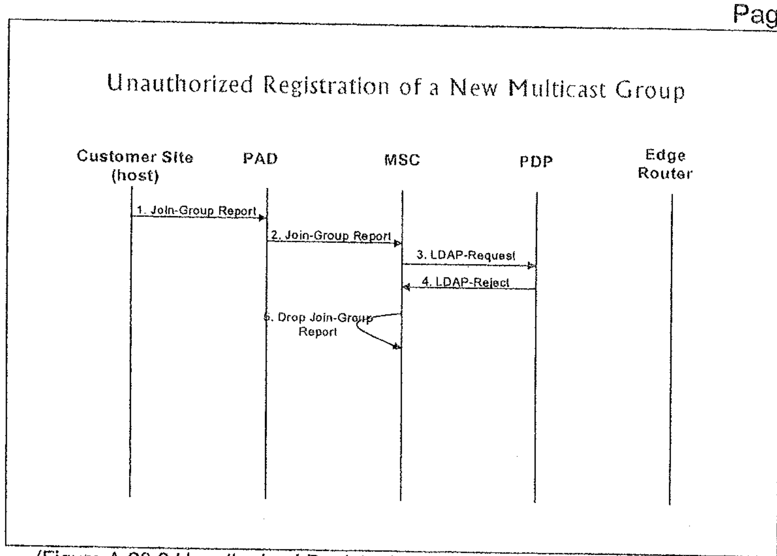
(1) Authorized Registration of a new multicast group
In the examples shown in figure A.20.1, a host on the customer site signals an IGMP join-group Report message to the edge router (1) (on the right hand side of figure A.20.1). IP filter in the PAD captures the IGMP messages based on PT=2. The PAD forwards the join-group Report message to the Multicast Service Controller (2) (MSC). The MSC queries the PDP within the policy database with LDAP or some other policy query protocol (3). The PDP finds the sender's IP address in the eligible membership list and approves that the sender join the group (4). The Membership Report message is forwarded to the edge router (5,6). In case the sender is the first member of that group on the network, the router adds the group being reported to the list of multicast group memberships on the network on which the sender is attached (7).



(Figure A.20.1 Authorized Registration of a new multicast group Example)

(2) Unauthorized Registration of a new multicast group
In the examples shown in figure A.20.2, a host on the customer site signals an IGMP join-group Report message to the edge router (1) (on the right hand side of figure A.20.2). The IP filter in the PAD captures the IGMP messages based on PT=2. The PAD forwards the join-group Report message to the Multicast Service Controller (2) (MSC). The MSC queries the PDP within the policy database with LDAP or some other policy query protocol (3). The PDP finds that the sender is not eligible to join the multicast group and rejects the join-group request (4). The MSC drops the join-group Report message and write into its event log a warning message (5). This prevents the unauthorized host from registering a new group in the edge router.

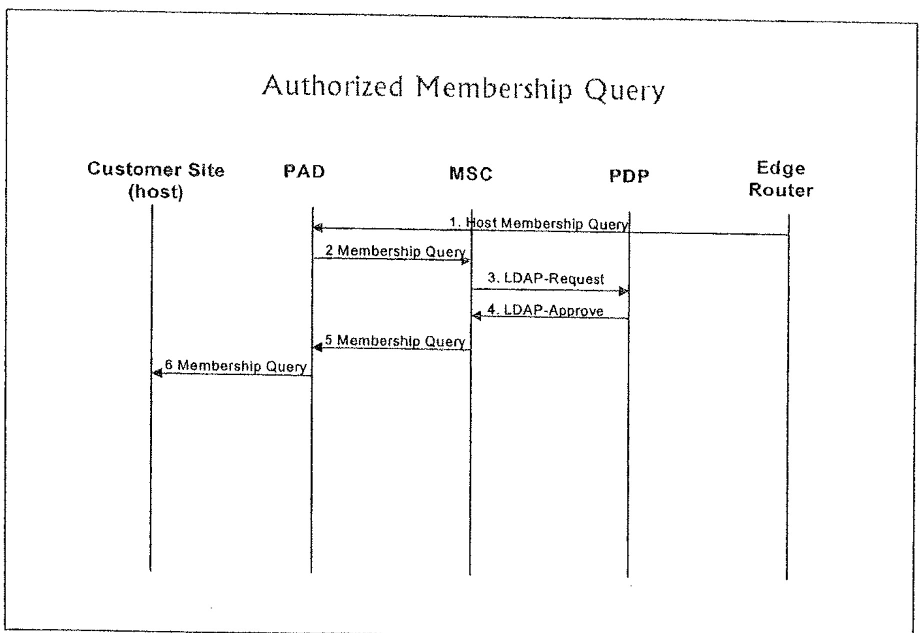
Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E. McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	



(Figure A.20.2 Unauthorized Registration of a new multicast group Example)

- Manage the host membership queries

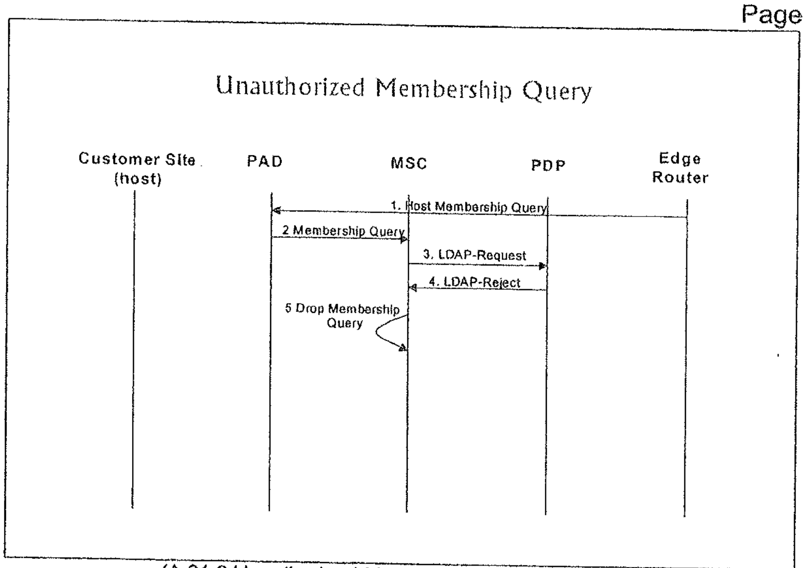
(1) Authorized Membership Query
In the example shown in figure A.21.1, the PAD receives an IGMP host membership Query message from the edge router (1). It passes the host membership Query message to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds the source address for this query is the authorized edge router and PDP approves the Query (4). The host membership Query message is forwarded to the hosts in the customer site/sub-network (5,6).



(A.21.1 Authorized Membership Query Example)

(2) Unauthorized Membership Query
In the example shown in figure A.21.2, the PAD receives an IGMP host membership Query message (1). It passes the host membership Query message to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the Query is from an unidentified or unauthorized source and rejects the Query (4). The MSC drops the Query message and writes a warning message into its event log (5). This prevents the denial of service attack by fake host membership Query messages.

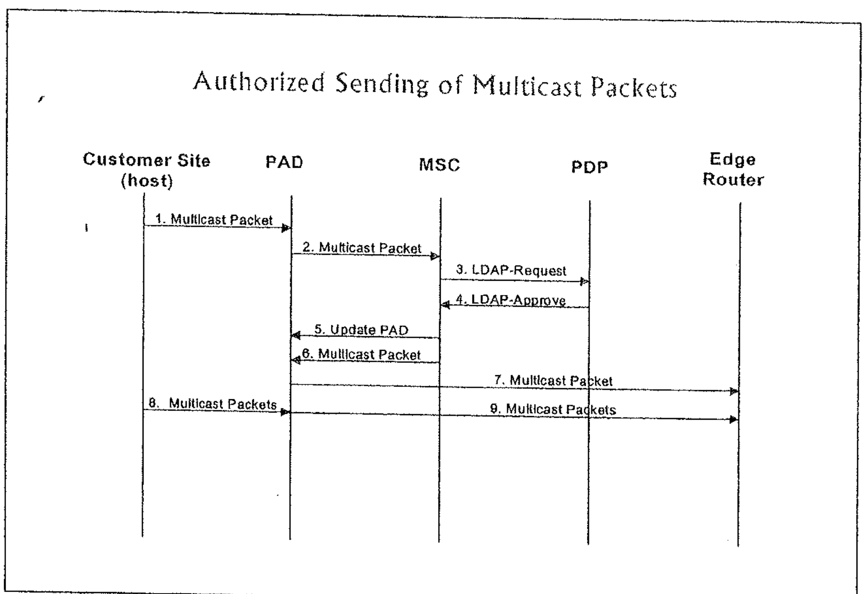
Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
David E McDysan	4/27/00	H. Lee Thomas	5/01/00	Lei Yao	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	



(A.21.2 Unauthorized Membership Query Example)

- Manage the sending of multicast packets to the network

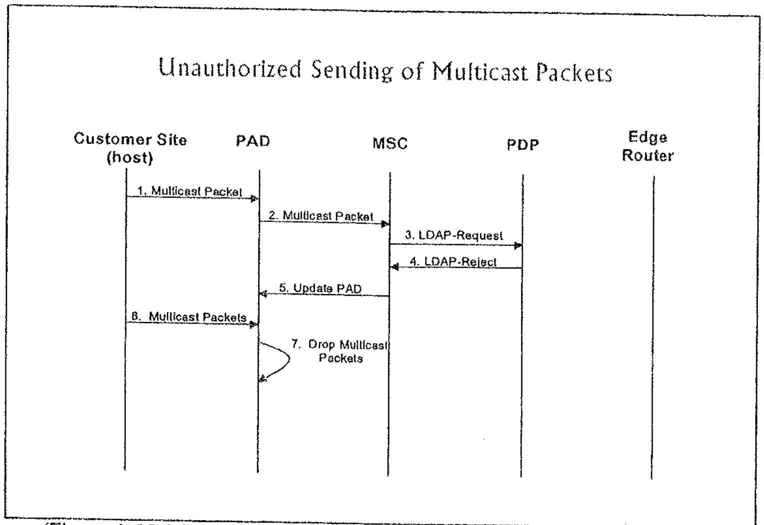
(1) Authorized sending of multicast packets to the network
In the example shown in figure A.22.1, a host on a customer site sends IP multicast packets to the multicast groups. When the PAD receives the first multicast packet (1), the IP filter captures the packet by checking its multicast address. The PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the source address of the IP multicast packet is authorized for sending multicast packets to the multicast group and approves the sending of the multicast packet (4). The MSC configures the PAD to directly forward multicast packets to the edge router for the (source, multicast address) pair (5) and returns the first multicast packet to the PAD (6). The PAD forwards the multicast packet to the edge router (7). The PDP forwards all the following multicast packets for the flow directly to the edge router without passing to the MSC (8,9).



(Figure A.22.1 Authorized sending of multicast packets Example)

(2) Unauthorized sending of multicast packets to the network
In the example shown in figure A.22.2, a host sends IP multicast packets to the multicast groups. When the PAD receives the first multicast packet (1), the IP filter captures the packet by checking its multicast address. The PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the source sending the multicast

packets is unidentified or unauthorized and rejects the sending of multicast packets to the network (4). The MSC configures the PAD to drop multicast packets for the (source, multicast address) pair and writes a warning message into the event log (5,6,7). This prevents the denial of service attack by flooding multicast packets onto the network.

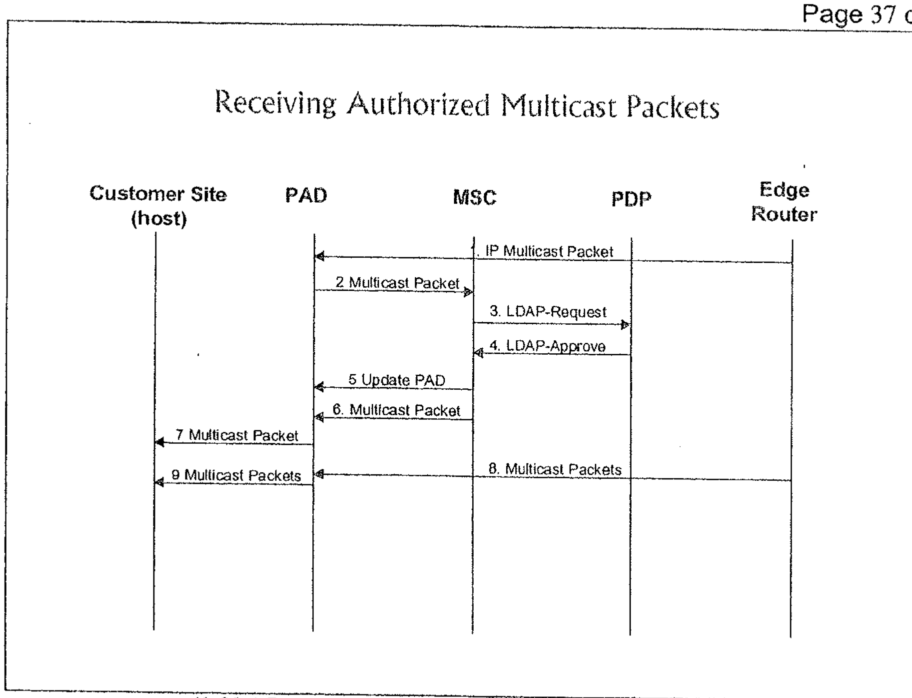


(Figure A.22.2 Unauthorized sending of multicast packets Example)

- Manage the receiving of multicast packets from the network

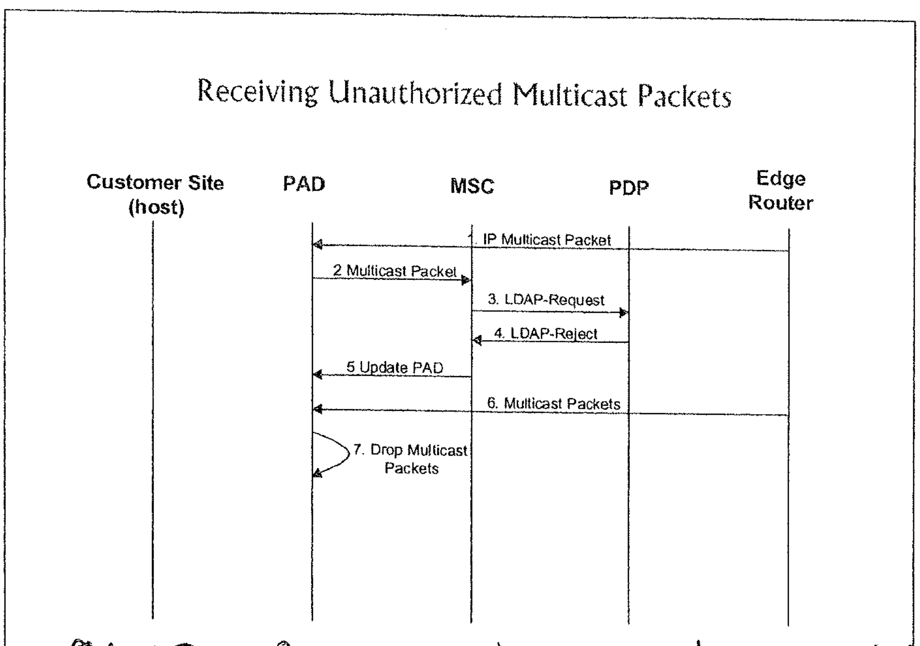
(1) Receiving authorized multicast packets
In the example shown in figure A.23.1, the edge router receives IP multicast packets from the network and forwards them to the PAD. When the PAD receives the first multicast packet from the edge router (1), the PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PDP finds that the source address of the IP multicast packet was authorized for sending multicast packets to the multicast group and approves forwarding the multicast packet to multicast hosts in the customer site (4). The MSC configures the PAD to directly forward to the edge router multicast packets for the (source, multicast address) pair (5), and returns the first multicast packet to the PAD (6). The PAD forwards the multicast packet to the multicast hosts in the customer site (7). The PAD forwards all the following multicast packets for the flow directly to the multicast hosts in the customer site without passing to the MSC (8,9).

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
[signature] 4/27/00	[signature] 5/01/00	[signature] 5/02/00
Print Name David E. McDysan	Print Name H. Lee Thomas	Print Name LEI YAO



(A.23.1 Receiving Authorized Multicast Packets Example)

(2) Receiving unauthorized multicast packets
In the example shown in figure A.23.2, the edge router receives IP multicast packets from the network and forwards them to the PAD. When the PAD receives the first multicast packet from the edge router (1), the PAD passes the packet to the MSC (2). The MSC queries the PDP with LDAP or some other policy query protocol (3). The PAP finds that the source sending the multicast packets is unidentified or not authorized and rejects forwarding the multicast packet to the multicast hosts in the customer site (4). The MSC configures the PAD to drop multicast packets for the (source, multicast address) pair and write a warning message into the event log (5,6,7). This prevents the unauthorized multicast packets from flooding the sub-network in the customer site.



(A 23.2 Receiving Unauthorized Multicast Packets Example)

Inventor Signature	Date	Inventor Signature	Date	Inventor Signature	Date
[signature]	4/27/00	[signature]	05/01/00	[signature]	5/02/00
Print Name David E. McDysan		Print Name H. Lee Thomas		Print Name LEI YAO	

ACRONYMS

ACK	Acknowledgement
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CCSC	Conference Call Service Controller
COPS	Common Open Policy Service
CPE	Customer Premise Equipment
CPU	Central Processor Unit
DA	Destination Address
Diffserv	Differentiated Services
DP	Destination Port Number
DSCP	Diffserv Codepoint
ECSC	E-Commerce Service Controller
FAST	First ATM SVC Trial
FIN	Finished
FR	Frame Relay
IGMP	Internet Group Multicast Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPTEL	IP Telephony
IPTELSC	IP Telephony Service Controller
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LPC	Linear Predictive Coding
LSP	Label Switched Path
MCIW	MCI WorldCom
MCRI	Message, Control, and Reporting Interface
MPLS	Multiprotocol Label Switching
MSC	Multicast Service Controller
PAD	Programmable Access Device
PADC	Programmable Access Device Controller
PANDSC	Programmable Access Device with Distributed Service Control
PDP	Policy Decision Point
PNNI	Private Network-Network Interface
POP	Point of Presence
PT	Protocol Type
PVC	Permanent Virtual Connection
QoS	Quality of Service
RBS	Reserved Bandwidth Service
RBSC	Reserved Bandwidth Service Controller
RST	Reset
RSVP	Resource Reservation Protocol
RTP	Real-time Transport Protocol
SA	Source Address
SBM	Subnet Bandwidth Manager
SC	Service Controller
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SP	Source Port Number
SPI	Service Policy Interface
SVC	Switched Virtual Connection
SYN	Synchronizing segment
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TOS	Type of Service
UDP	User Datagram Protocol
UNI	User Network Interface
WAP	Wireless Application Protocol

Inventor Signature Date	Inventor Signature Date	Inventor Signature Date
		Lei Yao 5/02/00
Print Name	Print Name	Print Name LEI YAO

Margo Livesay

From: Lei Yao [lei.yao@wcom.com]
Sent: Thursday, October 05, 2000 10:06 AM
To: 'Brian F. Russell'
Cc: 'Dave.mcdysan'; 'steven.mccann'; lee.thomas@wcom.com; jim.dalton@wcom.com
Subject: RE: patent application

ric.zip

Brian,

Attached please find our consolidated comments. We divided the comments into general comments and detailed comments. The general comments are put into a separate document. Detailed comments are made in the draft document with our initials. We also made some changes in the drawings.

Below is the conference bridge info.:
Date: 10/10
Time: 10:00 - 12:00 (EDT)
Toll Free - 888-455-9652
Pass Code 2562

Thanks again for your excellent work.

Lei

-----Original Message-----
From: Brian F. Russell [mailto:brussell@patentlawyers.com]
Sent: Tuesday, September 05, 2000 4:49 PM
To: lei.yao
Cc: Dave.mcdysan; steven.mccann
Subject: RE: patent application

<< File: RIC00033 (44796).doc >> << File: landscapedrawings.doc >> << File: portraitdrawings.doc >> Gentlemen,

Please find attached an initial draft of the first patent application. I would appreciate it if you could forward a copy to Lee for his review, as I don't have his email address.

I will continue working on the claims for the 3 additional applications while I await your comments. As you work through the document, please address the highlighted comments embedded in the text. Also, please consider whether the description is technically accurate and complete (whether it discloses to a person "skilled in the art" how to make and use the invention) and discloses the "best mode", if any, in which the invention may be used.

It would be helpful to me if comments for all the inventors can be compiled into either a single marked up version of the application or a single set of separate comments. Thank you for your assistance in the preparation of this application, and please contact me if I can resolve any issues that arise during the review process.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731

512.343.6116 (voice)
512.343.6002 (fax)
brussell@patentlawyers.com
www.patentlawyers.com

>>> Lei Yao <lei.yao@wcom.com> 09/05/00 02:33PM >>>
Brian,

Thanks for the update. We are looking forward to read the application.

Lei

-----Original Message-----
From: Brian F. Russell [mailto:brussell@patentlawyers.com]
Sent: Thursday, August 31, 2000 11:39 AM
To: lei.yao
Cc: Dave.mcdysan; steven.mccann
Subject: RE: patent application

Lei,
Just to update you on my progress on the applications, I have nearly completed a draft of the first application and expect to send you the draft for review next week. As we discussed, the all of the applications will contain the same basic description, but will differ in focus in the claims, summary and abstract. Hopefully, the commonality in the applications will facilitate your review.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
512.343.6116 (voice)
512.343.6002 (fax)
brussell@patentlawyers.com
www.patentlawyers.com

Margo Livesay

From: Brian F. Russell [brussell@patentlawyers.com]
Sent: Thursday, October 26, 2000 11:15 AM
To: dave.mcdysan; lei.yao
Cc: lee.thomas; steven.mccann
Subject: RE: patent application

Gentlemen,

Just to update you on the status of the patent applications, I have unfortunately been unable to work on the patent applications since I received the information Dave McDysan provided because of additional duties I have had to assume since Andrew, the firm's managing partner, broke his back last weekend.

Originally, I had anticipated completing all of the applications by the end of the month. I now believe that I can have revised drafts of the applications to you for review by 11/7/00.

I apologize for the delay.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
512.343.6116 (voice)
512.343.6002 (fax)
brussell@patentlawyers.com
www.patentlawyers.com

Margo Livesay

From:	Brian F. Russell [brussell@patentlawyers.com]
Sent:	Monday, November 06, 2000 11:35 PM
To:	dave.mcdysan; lei.yao
Cc:	lee.thomas; steven.mccann
Subject:	RE: patent application RIC00043

Follow Up Flag:	Follow up
Flag Status:	Completed

RIC00043.cla.doc

Gentlemen,
Attached please find the claims, abstract and summary for the external processor application.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
512.343.6116 (voice)
512.343.6002 (fax)
brussell@patentlawyers.com
www.patentlawyers.com

Margo Livesay

From:	Brian F. Russell [brussell@patentlawyers.com]
Sent:	Monday, November 06, 2000 11:40 AM
To:	dave.mcdysan; lei.yao
Cc:	lee.thomas; steven.mccann
Subject:	RE: patent application RIC00033
Follow Up Flag:	Follow up
Flag Status:	Completed

landscapedrawings.doc Overview.ppt portraitdrawings.doc RIC00033 (44796).doc RIC00042.cla.doc

Gentlemen,

Attached, please find attached the following:

(1) the second draft of the patent application, which includes your most recent comments [Please see my imbedded notes and questions pertaining to the "Overview" description that was added] and a full claim set;
(2) figures for the application (which are unchanged except for the insertion of reference numerals in the "Overview" drawings provided by Dave);
(3) claims, abstract and summary for the second application covering the PAD (Docket No. RIC00042).

I will send the claims, abstract and summary for the other two applications either later today or tomorrow.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
512.343.6116 (voice)
512.343.6002 (fax)
brussell@patentlawyers.com
www.patentlawyers.com

Margo Livesay

From:	LEI YAO [lei.yao@wcom.com]
Sent:	Wednesday, November 08, 2000 2:27 PM
To:	'Brian F. Russell'; dave.mcdysan
Cc:	lee.thomas; steven.mccann
Subject:	RE: patent application RIC00044

Brian,

Thanks for putting together all four applications during the short period.

Steven,

I will coordinate with Dave and Lee to review these applications. After the applications have been agreed on by us, do we need approval from you before we really submit these applications? What is the next step from the legal department?

Thanks.
Lei

-----Original Message-----
From: Brian F. Russell [SMTP:brussell@patentlawyers.com]
Sent: Wednesday, November 08, 2000 12:37 AM
To: dave.mcdysan; lei.yao
Cc: lee.thomas; steven.mccann
Subject: RE: patent application RIC00044

<< File: RIC00044.cla.doc >> Gentlemen,

Please find attached the claims for the final patent appliication covering the MCRI.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
512.343.6116 (voice)
512.343.6002 (fax)
brussell@patentlawyers.com
www.patentlawyers.com

Margo Livesay

From: LEI YAO [lei.yao@wcom.com]
Sent: Tuesday, November 21, 2000 7:11 PM
To: 'paul.roberts@wcom.com'; 'Steven.McCann@wcom.com'
Cc: 'dave.mcdysan@wcom.com'; 'brussell@fbvgd.com'; 'lee.thomas@wcom.com'
Subject: patent applications

patentcmts.zip

Paul,

Attached please find the final comments we made for the patent applications prepared by Brian Russell. We understand that you will work on this case representing Steven. The applications were well written. We only made several minor changes. If you turn on "track change" options of MS Words, you should be able to see those changes. We believe that the applications are ready to be submitted. Since there is going to have a patent law change on 11/29, which may bring negative impacts on pending patents, we probably would like to submit these patent applications before that date to better serve the company's interests.

Please let us know your thoughts.

Thank you very much.
Lei

Margo Livesay

From: Brian F. Russell [brussell@patentlawyers.com]
Sent: Wednesday, November 22, 2000 11:45 AM
To: lei.yao
Cc: dave.mcdysan; lee.thomas; Paul.roberts
Subject: Re: Patent applications

Gentlemen,

Thank you for your assistance in preparing the patent applications. I have reviewed the comments you had and have finished incorporating them into the applications.

To speed up preparation of the legal documents that will accompany the applications, I need updated addresses for each of you (the ones listed in the disclosure seem to be out of date).

Thank you for your help.

Best regards,

Brian F. Russell
Felsman, Bradley, Vaden, Gunter & Dillon, LLP
Suite 350, Lakewood on the Park
7600B N. Capital of Texas Hwy.
Austin, TX 78731
512.343.6116 (voice)
512.343.6002 (fax)
brussell@patentlawyers.com
www.patentlawyers.com

Patent Docket No.: **RIC00043**

DECLARATION AND POWER OF ATTORNEY FOR UTILITY PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

External Processor For A Distributed Network Access System

the specification of which

___ is attached hereto
_X_ was filed on November 28, 2000
as Application Serial No. 09/723,501
___ and was amended on

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof of more than one year prior to this application, and said invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code §119 (a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed
______	______	______	____ yes ____ no
(number)	(country)	(date filed)	

EXHIBIT N

Patent Docket No.: **RIC00043**

I hereby claim the benefit under Title 35, United States Code§119(e) of any United States provisional application(s) listed below.

(Application Number(s)) (Filing Date mm/dd/yy)

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) or Section365(c) of any PCT international application designating the United States of America, listed below, and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Filing date) (Status)

I hereby appoint Steven McCann, Reg. No. 34,958; Paul A. Roberts, Reg. No. 40,289; Michael B. Chernoff, Reg. No. 42.408; Suresh Koshy, Reg. No. 42,761; Brian C. Oakes, Reg. No. 41, 467;; Andrew J. Dillon, Reg. No. 29,634; Brian F. Russell, Reg. No. 40,796; Matthew W. Baca, Reg. No. 42,277; Antony P. Ng, Reg. No. 43,427; Richard McCain, Reg. No. 43,785; and Michael E. Noe, Jr., Reg. No. 44,975 my attorneys and Frank A. McKiel, Reg. No. 43,792 my patent agent with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send future correspondence to:
Technology Law Department
MCI WORLDCOM, Inc.
1133 19th STREET NW
WASHINGTON, D.C. 20036

Direct Telephone Calls To:
(202) 736-6604

I hereby declare that all statements made herein of my knowledge are true and that all statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of Sole or First Inventor: **Dave McDysan**
P.O./Residence Address: 2159 Astoria Circle, #104, Herndon, VA 20170
Citizenship: United States of America

Signature: Dave McDysan Date: Jan 17, 2001

Full name of Additional Joint Inventor, if any: **Howard Lee Thomas**
P.O./Residence Address: 325 Woodmar Court, Ballwin, MO 63311
Citizenship: United States of America

Signature: ______________________ Date: ______________

EXHIBIT N

Patent Docket No.: **RIC00043**

Full name of Additional Joint Inventor, if any: Lei Yao
P.O./Residence Address: 2000 S. Eads Street, #517, Arlington, VA 22202
Citizenship: China

Signature: Lei Yao Date: 01/17/2001

EXHIBIT N

Patent Docket No.: **RIC00043**

DECLARATION AND POWER OF ATTORNEY FOR UTILITY PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

External Processor For A Distributed Network Access System

the specification of which

___is attached hereto
X was filed on November 28, 2000
as Application Serial No. 09/723,501
___ and was amended on

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof of more than one year prior to this application, and said invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code §119 (a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed
______	______	______	____ yes ____ no
(number)	(country)	(date filed)	

EXHIBIT N

Patent Docket No.: **RIC00043**

I hereby claim the benefit under Title 35, United States Code§119(e) of any United States provisional application(s) listed below.

(Application Number(s)) (Filing Date mm/dd/yy)

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) or Section365(c) of any PCT international application designating the United States of America, listed below, and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Filing date) (Status)

I hereby appoint Steven McCann, Reg. No. 34,958; Paul A. Roberts, Reg. No. 40,289; Michael B. Chernoff, Reg. No. 42.408; Suresh Koshy, Reg. No. 42,761; Brian C. Oakes, Reg. No. 41, 467;; Andrew J. Dillon, Reg. No. 29,634; Brian F. Russell, Reg. No. 40,796; Matthew W. Baca, Reg. No. 42,277; Antony P. Ng, Reg. No. 43,427; Richard McCain, Reg. No. 43,785; and Michael E. Noe, Jr., Reg. No. 44,975 my attorneys and Frank A. McKiel, Reg. No. 43,792 my patent agent with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send future correspondence to:
Technology Law Department
MCI WORLDCOM, Inc.
1133 19th STREET NW
WASHINGTON, D.C. 20036

Direct Telephone Calls To:
(202) 736-6604

I hereby declare that all statements made herein of my knowledge are true and that all statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of Sole or First Inventor: **Dave McDysan**
P.O./Residence Address: 2159 Astoria Circle, #104, Herndon, VA 20170
Citizenship: United States of America

Signature: ______________________ Date: ______________

Full name of Additional Joint Inventor, if any: **Howard Lee Thomas**
P.O./Residence Address: 325 Woodmar Court, Ballwin, MO ~~63311~~ 63011 HLT 12/22/00
Citizenship: United States of America

Signature: H Lee Thomas Date: 12/22/00

EXHIBIT N

Full name of Additional Joint Inventor, if any: **Lei Yao**
P.O./Residence Address: 2000 S. Eads Street, #517, Arlington, VA 22202
Citizenship: China

Signature: ______________________________ Date: ____________________

EXHIBIT N